Analyzing of legitimate interest under the General Data Protection Regulation in the light of the Court of Justice of the European Union and the European Court of Human Rights case law

by

İREM MUTLU

Master of Law

in

Social Science and Humanities

KOÇ
ÜNİVERSİTESİ

April 12, 2023

Analyzing of legitimate interest under the General Data Protection Regulation in the light of the Court of Justice of the European Union and the European Court of Human Rights case law

Koç University

Graduate School of Sciences and Engineering

This is to certify that I have examined this copy of a master's thesis by

İREM MUTLU

and have found that it is complete and satisfactory in all respects,

and that any and all revisions required by the final

examining committee have been made.

Committee Members:

_____

Prof. Bertil Emrah ODER

_____

Assoc. Prof. Sezen Kama IŞIK

_____

Assist. Prof. Demet Çelik ULUSOY

Date: _____

[To my home]

ABSTRACT

Analyzing of legitimate interest under the General Data Protection Regulation in the light of the Court of Justice of the European Union and the European Court of Human Rights case law

İREM MUTLU

Master of Law in Social Science and Humanities

April 2023

Legitimate interest is one of the most intriguing and ambiguous subjects under data protection law. It is difficult to define as a notion and its repercussions in practice cannot be easily anticipated. The goal of the present thesis is to investigate whether legitimate interest clause under the General Data Protection Regulation (GDPR) provides an effective protection. To answer this question, first, circumstances that created the GDPR and the reasons why it was needed are explained from the legitimate interest perspective. Second, the consequences of the lack of legal certainty caused by the legitimate interest clause are pointed out. Third, benchmarks are drawn up for an optimum balance testing by specifying which elements should be considered in a legitimate interest review one by one. Since the case law of both CJEU and ECtHR play a critical role in ensuring legal certainty, related landmark cases are examined in a comparative way. Lastly, a legal projection of what awaits the legitimate interest in the future is demonstrated with the help of the Article 29 Working Party opinions, national data protection authorities' decisions and international guidelines and recommendations.

Keywords: legitimate interest, data protection, data controller, data subject, privacy, Court of Justice of the European Union, European Court of Human Rights, legal certainty, necessity, balancing exercise, additional safeguards, proportionality, transparency.

ÖZETÇE

Avrupa Birliği Adalet Divanı ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Genel Veri Koruma Tüzüğü Kapsamında Meşru Menfaatin Analizi

İREM MUTLU

Kamu Hukuku, Yüksek Lisans

Şubat 2023

Meşru menfaat, veri koruma hukuku kapsamında en merak uyandıran ve muğlak konulardan biri olup, tanımlanması zor ve pratikteki yansımaları kolayca tahmin edilemez bir kavrama karşılık gelmektedir. İşbu tezin amacı, Avrupa Birliği Genel Veri Koruma Tüzüğü (GKVT) kapsamındaki meşru menfaat hükmünün etkili bir koruma sağlayıp sağlamadığını araştırmaktır. Bu soruyu cevaplamak için öncelikle GKVT'yi oluşturan koşullar ve GKVT'ye neden ihtiyaç duyulduğu, meşru menfaat perspektifinden açıklanmaktadır. İkinci olarak, meşru menfaat hükmünün yol açtığı hukuki belirlilik eksikliğinin sonuçlarına işaret edilmektedir. Üçüncü olarak, meşru menfaat incelemesinde hangi unsurların dikkate alınması gerektiği tek tek belirtilerek optimum bir denge testi için kıstaslar oluşturulmaktadır. Hem Avrupa Birliği Adalet Divanı hem de Avrupa İnsan Hakları Mahkemesi içtihatları hukuki kesinliğin sağlanmasında kritik bir rol oynadığından, konuya ilişkin öncü davalar karşılaştırmalı olarak incelenmektedir. Son olarak, 29. Madde Çalışma Grubu görüşleri, ulusal veri koruma makamlarının kararları, uluslararası yönergeler ve tavsiyeler yardımıyla gelecekte meşru menfaati neyin beklediğine ilişkin hukuki öngörü ortaya konmaktadır.

Anahtar Kelimeler: meşru menfaat, veri koruma, veri sorumlusu, ilgili kişi, mahremiyet, Avrupa Birliği Adalet Divanı, Avrupa İnsan Hakları Mahkemesi, hukuki belirlilik, gereklilik, denge testi, ek tedbirler, orantılılık, şeffaflık.

AKNOWLEDGEMENTS

I would like to express my gratitude to my advisor, Prof. Dr. Bertil Emrah ODER for her invaluable advice and guidance on my thesis. I would also like to thank to The Scientific and Technological Research Council of Türkiye (TUBITAK) for financially supporting my master's degree within the scope of 2210-A domestic general master's scholarship.

I am sincerely grateful to my family, for their trust and belief in me. The completion of this study could not have been possible without them.

TABLE OF CONTENTS

ABBREVIATIONS

CJEU	Court of Justice of the European Union
Commission	European Commission
DPA	Data Protection Authority
Directive	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
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
EU	European Union
GDPR(Regulation)	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data
OECD	Organization for Economic Co-operation and Development
TFEU	Treaty on the Functioning of the European Union
UN	The United Nations
WP29	The Article 29 Working Party

Chapter 1:
INTRODUCTION

In 2009, the European Union Consumer Commissioner termed personal data as "the new oil".[1] This terminology shows evidently that the States have informational appetite to become a huge political and economic power processing personal data. The tasks of public sector agencies such as war on terror or surveillance schemes of national security deduct from the emergence of the welfare state and relate directly to the processing of personal data. Not only the public sector agencies, but also a rapidly growing market in private sector trading customers' personal data creates an Internet economy which is fueled by personal data.

Bygrave sees these developments as a catalyzer of the appearance of the significance of the field, since data protection law aiming to regulate the exploitation of personal data stands in the way of administrative, commercial, or social processes.[2] Therefore, the normative nature of the field consists of one of the most significant counterbalances to the digital world's priorities such as increased organizational efficiency and maximization of financial profit.[3] On the contrary, it is undeniable that regulating in the data protection field is deemed to be a challenge to the states given the difficulties to define the notions of data, protection and privacy considering different constitutional orders, legal systems, and interpretations among different countries. The difficulties of making the risk assessment to predict how risky to provide personal data to an entity or organization, the rights of the individual in relation to the benefit of society, transparency and assigning accountability can be shown among other personal data challenges of today. In case that important services are denied when people are unwilling to supply that data whether or not individuals have a real choice is another matter of discussion.[4]

[1] Future of Privacy Forum and Nymity innovating compliance, Processing Personal Data on the Basis of Legitimate Interests under the GDPR Practical Cases, (Sep. 4, 2022), https://www.ejtn.eu/PageFiles/17861/Deciphering_Legitimate_Interests_Under_the_GDPR%20(1).pdf.

[2] LEE A. BYGRAVE, DATA PRIVACY LAW AN INTERNATIONAL PERSPECTIVE 9 (2014).

[3] Id. at 5.

[4] Neil Robinson et al., *Review of the European Data Protection Directive* (May,2009), https://ico.org.uk/media/about-the-ico/documents/1042349/review-of-eu-dp-directive.pdf.

Data protection field reveals its objectives with the name itself. The name of this field is not personal data law, but personal data protection law. The literal meaning of the protection is the condition or state of being kept safe from injury, damage, or loss. Then, why is personal data damaged and who creates this situation? Why does data need to be protected? The reason behind that data is considered under the threat of misusing by natural and legal persons. On the one hand, the processing of data, as a rule, is not a prohibited activity and data is naturally processed in every area of our lives. On the other hand, the exponential increase of processed data in recent decades raises the key question is whether data is fairly and legitimately processed. What data can we process and under which conditions? Unfortunately, these questions do not consist of the easiest questions to answer and different answers to this question given by countries may result in completely different applications. According to Hustinx, "Data protection law was not designed to prevent the processing of such information or to limit the use of information technology per se, instead, it was designed to provide safeguards whenever information technology would be used for processing information."[5] Today, as Lynskey described, "a tug of war" in which power and trumps are constantly changing direction between the parties is being witnessed for control over personal data between individuals and public or private organizations.[6]

From general policy perspective, two distinct ways exist to formulate the policy answers by countries. The first is the protection system like EU's method restricting the amount of data collected and preventing that collected data from being processed, and the second is US's approach assuming data collection is acceptable and potentially beneficial and legislating only where certain abuses occur.[7] This thesis will focus on the EU's perspective in the field which creates its own data protection law with specific legal instruments to ensure that data is not collected excessively, and it cannot be used for specified purpose during the collection of data.

[5] Peter Hustinx, *EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation,* (Sep 15, 2014), https://edps.europa.eu/sites/default/files/publication/14-09-15_article_eui_en.pdf.

[6] ORLA LYNSKEY, THE FOUNDATIONS OF EU DATA PROTECTION LAW 14-45, (2015).

[7] DOROTHEE HEISENBERG, NEGOTIATING PRIVACY, The European Union, the United States, and Personal Data Protection 14, (2005).

First of all, it is aimed to explore the appearance of the notion of legitimate interest in international texts and finally stated in Article 6/1/(f) of GDPR spotting among other legal grounds of legitimate processing of data in this study. Despite the various essays and opinions on other grounds, the legitimate interest of the data controller has not been at the spotlight given that other grounds have more straightforward requirements comparing legitimate interest. Therefore, it is not shocking that the authorities and academics hesitate to discuss in depth the ground of legitimate interest considering its flexible nature. On the other hand, looking at the practices of data controllers, it is seen that the legitimate interest, which has become a frequently applied legal ground by data controllers and this trend is likely to continue with GDPR.

The main problem that this thesis will deal with is the lack of legal certainty of legitimate interests under GDPR. Since the European Union has taken an important step with the GDPR on uniformity, GDPR constitutes a critical legal tool and starting point for this thesis's subjects. Yet, in a century where regulations cannot capture technology it is needed a holistic approach to develop a better understanding on the issue.

It is aimed to address the question of how to maintain the critical balance between the legitimate interest of the data controllers and the rights of the data subjects or third parties. Unfortunately, the balancing exercise inevitably involves subjective elements, and it is difficult to incorporate it into a concrete and tangible test. As Wrigley pointed out, vague power result in vague responsibility and it is also a matter of curiosity how the abuse of the clause can be prevented.[8] At this point, the Court of Justice of European Union and the European Court of Human Rights case law will step in to lead the way. The latter one will also help to position the right to respect private life in the context. Nevertheless, to date, decisions made by the local or international courts establish only a starting point and are not enough to cope with possible future challenges such as profiling or behavioral advertising. Legitimate interest can be seen as a guarantor of

[8] Sam Wrigley, *Bots and AI-Related Technologies, Legitimate Interest, And Fair Processing under The General Data Protection Regulation,* (Dec 17, 2021), https://helda.helsinki.fi/bitstream/handle/10138/336786/wrigley_sam_dissertation_2021.pdf?sequence=1&isAllowed=y.

GDPR's future-proof and technology neutral character enabling ongoing delivery and improvement of products and services by ensuring the protection of fundamental rights and freedoms of data subjects. On the other side, its misinterpretation or application in bad faith may cause the legitimate interest clause to be seen as a loophole and abused. Therefore, it is indispensable to investigate how the technological developments will affect the legitimate interest approach.

In conclusion, this thesis will set out to evaluate international texts and case law as legal instruments on the questioning optimum balancing exercise in the context of legitimate interest. Interrogating whether legitimate interest clause provides an effective protection, the birth and historical development of the concept of legitimate interest will be examined and it will be revealed that it actually takes its source from the principles of fairness and lawfulness. It will be seen that the examination of legitimate interest is not a simple pro cons test, and it can be misleading to give answers within the general rules and patterns by showing that all the conditions are reviewed. It will be tried to show that the plaster holding the bricks of the legitimate interest building together is the purpose limitation, transparency and proportionality, and that additional safeguards are essential to increase the earthquake resistance of the building. After developing a sound understanding of these elements constituting legitimate interests, literature and case law analyzes will be made regarding the lack of legal certainty, which is the biggest problem to be dealt with. In the last part of the study, it will be stated that this problem can reach endless dimensions in fraud detection and blacklist issues with the increase in digital records; it will be based on the prediction that future threats such as direct marketing, profiling, behavioral advertising can grow like a snowball and move away from effective protection.

Chapter 2: APPEARANCE OF THE NOTION: BACKDROP AND CONTEXTUALIZATION

2.1 Historical Background

This section's main objective is to demonstrate the backdrop of the notion of legitimate interest and its concept in EU law. However, due to the fact that the concept of legitimate interest parallels the development of the concept of personal data protection in many ways, it is inevitable to touch upon the development of personal data law when examining the appearance of legitimate interest.

In the concept of data protection law, the doctrine focuses mainly on three different orientations of regulation in the world.[9] Enacting a general data protection law, as in Europe, is considered the first of this taxonomy. While the USA prefers to introduce different laws regarding the different sectors protecting private life, in Latin American countries such as Brazil, Peru and Argentina the notion of "habeas data" has revealed which can be considered a type of individual complaint. It is important to observe the place of Europe among other orientations and discover the reasons for this choice. However, since this thesis analyzes legitimate interest in the European approach, the other methods will not be examined in further details and it will be continued to focus on the emergence of the concept in Europe.

In Europe, the development of automatic data processing technology forms the starting point of the discussions about the threats to the right to privacy in the late 1960's. As can be deduced from the first legal texts, the central database preparations of the states were the trigger element in the context of personal data protection.[10] During the period that some authors call the "first-generation data protection laws", it has been a process aimed at maintaining a balance against the disproportionate use of centralized and far-reaching data acquisition power by states that outweigh the individual. As

9 SEZEN KAMA IŞIK, AVRUPA VERİ KORUMA HUKUKUNA ANAYASAL BİR BAKIŞ 56, (2020).

10 ELİF KÜZECİ, KİŞİSEL VERİLERİN KORUNMASI 126, (2021).

another key point of this stage, it is concentrated on the data processed by computers and the anxiety caused by the loss of control can be felt in the legal actions taken.[11] Using data for purposes other than the purposes which it was collected, the potential for misinterpretation and misapplication of data and automatization of decision-making process caused the growing complexity and diminishing transparency from the individuals' point of view under the name of data subjects. The repression of authoritarian regimes, political scandals, and dystopian literature undeniably contributed to feeding these fears.[12]

Auditability and transparency have been the most emphasized principles to find an optimum balance and create the separation of informational powers between states and individuals.[13] Consequently, the most critical dynamic behind the law of the State Hessen, considered as the oldest data protection regulation, is the possible effects of the establishment of a central data bank at the federal level on the right to privacy.

It was necessary to wait until the end of 1970's for the right to personal data protection to gain a human rights perspective instead of technology centric approach. It becomes clear with the establishment of many data banks in both the public and private sectors that state dominance in the field of data processing is not the only problem faced and a more obvious and tangible danger exists requiring the request for the right to data protection. The constitutions of Portugal and Spain opened a new door as the most important indicator that the issue is being discussed on the human rights axis taking its source from the right to privacy. [14,15] Other European countries followed the similar path recognizing the data protection at the constitutional level. At this point, it should be noted that although a subjective right of defense obtained by the struggle of an individual has been established in the aforementioned period, the rights that an individual has in this area are limited to the right to access data in existing data banks and correct inaccuracies of data processing. It took until the mid-1980s for the "prevent attack" perspective to be seen as not sufficient to address the issue and for the individual

[11] Council of Europe, *New Technologies: A challenge to privacy protection*?, (Jan 20, 1988), https://rm.coe.int/09000016809125af.
[12] BYGRAVE, supra note 2, at 10.
[13] KÜZECİ, supra note 10, at 221.
[14] PORTUGAL'S CONSTITUTION. art.35.
[15] SPANISH CONSTITUTION. art.18.

to be able to decide which of their data to process and to determine the future of information. The justification of "Volkzählung" decision of the German Constitutional Court demonstrates that the protection of personal data has now come to be recognized as an area where an individual actively participates in all stages of the data processing process and where the authorities have certain obligations in this regard.[16] It is not by chance that the introduction of international texts in the field of personal data protection also coincided with the 1980s since the organizations such as UN, OECD and Council of Europe have realized that the issue has ceased to be a national issue and has become an international issue especially when the transfer of personal data comes into play. It can be observed that the Council of Europe emphasizes in its first legal texts that the remote collection of personal data by automatic means, where the data subject plays no active part in the data processing typically cause in the data subject's lack of knowledge of when the data are collected on him and what sort of data are collected.[17]

As a result of the developments in information technologies in the 1990s, when the diversity of services and products increased with an insurmountable momentum, the following question arose when the threat on personal data outweighed the guarantees provided to the individual: How to ensure international protection without interfering with the free flow of information?[18] In fact, easy producing, editing, disseminating, and storing of personal data with a decreasing cost ensured the personal data is considered a commodity and hence it could not escape from the attention of regulatory bodies.[19] Although the country-based and local breakthroughs described so far for the formation of the general legal basis have been shown, the dynamic structure of personal data law for the whole world is a big challenge and it is not possible to say that it develops in the same way everywhere. The different levels of sensitivity of the states to technological developments, which have become such an integral part of daily life, necessitated the discussion of the issue at a supranational level in order to ensure the protection of personal data effectively, regardless of the country's practice. The Directive, which will be examined in detail below, has the feature of a turning point in its field as the most

[16] Abstract of the BVerfG [German Federal Constitutional Court] Dec. 15, 1983, 1 BvR 209, 269, 362, 420, 440, 484/83, https://www.datenschutz.rlp.de/fileadmin/lfdi/Dokumente/Gerichtsurteile_und_-beschluesse/bverfge_65_1_-_volkszaehlung.pdf.

[17] Council of Europe, supra note 11.

[18] KÜZECİ, supra note 10, at 126.

[19] LYNSKEY, supra note 6.

compelling model on the subject so far with an impact that goes beyond the EU borders at this point.[20]

After briefly evaluating certain milestones in the development of personal data protection law, the international sources of this law will be examined, yet since the subject of this thesis is limited to the concept of legitimate interests, these international sources will also be analyzed within the framework of the development of this concept. The WP29, in its Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC relates the notion of legitimate interest to the broader principle named "lawfulness". [21] Lawfulness incorporates the fact that data processing should be based on legal grounds which appears firstly as an exception to privacy rights and then comes into the picture as an independent requirement in the context of data protection. Therefore, WP29 bases the history of this concept on the Article 8 of the ECHR. The Article 8 stipulates that the interference with the right of privacy is prohibited by rule except strictly defined conditions. Although the Article 8 does not refer to the data protection, it cannot be ignored the contribution to the data protection law considering the case law of the Strasbourg court which expands the meaning of the Article 8 protecting privacy to cover data protection interests. In the context of legitimate interest, assessing the element of necessity in a democratic society under this article requires that the interference has a legitimate purpose as a prerequisite.

The Council of Europe's Convention 108 for the Protection of Individuals with regard to automatic processing of personal data prepared is an early framework for the separation of the concept of data protection from the interference with privacy. [22] Even though the Article 5 of the Convention envisages the principle of obtaining data undergoing automatic processing fairly and lawfully listed in the first place among other fundamental principles of data protection law, it did not give further details for other legal grounds of data processing. Nonetheless, the fact that the concept of "personal data" is defined as "any information relating to an identified or identifiable

[20] KÜZECİ, supra note 10, at 127.
[21] Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, 844/14/EN WP 217 (Apr. 9, 2014) [hereinafter OPINION].
[22] The Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Jan. 28, 1981, E.T.S. 108, https://rm.coe.int/1680078b37 [hereinafter Convention 108].

individual" revealed that the concepts of privacy and personal data differ from each other.

A few months before Convention 108 was adopted, the OECD adopted Guidelines on the Protection of Privacy and Transborder Flows of Personal Data[23] on 23 September 1980 (updated in 2013) which constitutes one of the international non-binding sources in the data protection context. The Guidelines aims to in parallel with Convention 108 help to harmonize national privacy legislation on the one hand protecting human rights and on the other hand preventing interruptions in international flows of data providing a consensus on basic principles applicable in different national legislations. It provides "collection limitation principle" stated in Article 7 which stipulates that personal data "should be obtained by lawful and fair means, where appropriate, with the knowledge or consent of the data subject." Here, consent is considered an option to be used among other legal grounds after the appreciation of the interests and rights at stake according to the WP29. As a meaningful difference compared to Convention 108, the scope of the OECD Guidelines was limited to personal data "which because of the manner in which they are processed, or because of their nature or the context in which they are used, pose a danger to privacy and individual liberties." Hustinx states, "the notion of 'risk' as a threshold condition for protection was not entirely compatible with the fundamental rights-based approach of the Council or Europe. In addition, "the need for a legitimate purpose and a lawful basis for processing of personal data per se was absent in the Guidelines."[24]

The concept of legitimate interest is used for the first time in its present meaning in the Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals regarding the processing of personal data and on the free movement of such data. As it is known, the European Union, despite its multinational structure, has reached a structure defined as supranational as a result of the transfer of the sovereign authority of the Member States. This structure, which aims to establish an integrated Europe, has supported its political and legal evolution with basic

[23] Organization for Economic Cooperation and Development (OECD), Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (Sept. 23, 1980), https://www.oecd-ilibrary.org/docserver/9789264196391-en.pdf?expires=1664894751&id=id&accname=guest&checksum=E1E15F65ECD21C2AC345C4C4BBC1700C [hereinafter OECD Guidelines].

[24] Hustinx, supra note 5, at 2.

principles such as human rights and the rule of law, following the necessities of the time, the increase in the number of its members and its economic integration. As one of the most important objectives stated in the Single European Act, the Directive was intended to ensure the protection of personal data privacy while securing economic benefits on the one hand, to establish a common internal market and not to harm the freedom of persons, services and capital in this market with an agreement at a Union level.[25]

Article 7 (f) of the Directive recognizes legitimate interest as one of the legal grounds of legitimate data processing derogating that these interests are overridden by the interests for fundamental rights and freedoms of the data subject. The journey of the Directive from the drafts to the final text will be analyzed in further chapters in detail, however it can be concluded that with the *ASNEF and FECEMD* judgment, the direct effect of the legitimate interest under Article 7 (f) was recognized by the CJEU. [26] In the judgment, the Court underlines that Member States are not entitled to impose additional unilateral restrictions and requirements regarding the legal grounds such as Article 7 (f) for lawful data processing in domestic law and the margin of appreciation by states is limited in this respect. The fact that the Spanish Royal Decree brought the obligation of the data controller to process personal data that appear in public sources as an additional condition to benefit from the legitimate interest ground was seen in breach of the Directive since such restriction means a barrier to the free movement of personal data. The second preliminary question is whether Article 7(f) of the Directive has direct effect, and the Court gives a positive answer and gives a further explanation on the relationship between the data subject's rights of Articles 7 and 8 of the Charter of Fundamental Rights of the European Union and includes the right for respect for private and family life in the scope of the balancing. Along with the Lisbon Treaty[27] in 2009 which gives the Charter [28] the same legal value as the Treaties, it is reinforced that the protection of personal data is situated separately under fundamental rights as

[25] EMİNE HİZARCİ, 6698 SAYILI KİŞİSEL VERİLERİN KORUNMASI KANUNUNUN AB VERİ KORUMA HUKUKU IŞIĞINDA DEĞERLENDİRİLMESİ 44, (2020).

[26] Joined Cases C-468/10 and C-469/10, Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) (C-468/10) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) (C-469/10) v Administración del Estado, 2011 E.C.R. I-12181.

[27] Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community, Dec. 13, 2007, 2007 O.J. (C 306) 1.

[28] Charter of Fundamental Rights of the European Union, art. 51(1), 2000 O.J. C 364/01.

stated in Article 8. It requires a legitimate basis which can be the basis of consent or other legitimate basis prescribed by law for the data processing. The fact that the provision deals with the protection of personal data not under the umbrella of respect of private and family life, but under a specific category of fundamental right demonstrates the significant shift to the right-approach on the data protection. The right to protection of personal data is not an absolute right, therefore it should be read in combination with Article 52 of Charter which regulates that limitations need to be necessary, proportionate, provided by law and respect the essence of the right. Since the EU data protection legislation has its basis in the EU primary law which covers Article 16 of TFEU and the Charter, any constraints on right to protection of personal data cannot go further than the conditions under Article 8 and 52 of the Charter.[29]

The legal instruments in respect of data protection in the European Union share two common roles. Firstly, the role of harmonization of national laws aims to realize a minimum standard of protection and in the meantime, the maintenance of the free trans-border flow of personal data which constitutes one of the main European Union's goals; secondly, the role of the balance the individuals' interests against societal and business interests in the free movement and availability of data. However, the margin of discretion of states applying these legal instruments differ from each other. While OECD Guidelines and Convention 108 provide an extensive margin of manoeuvre for States and only frames general principles in data protection law, the Directive 95/46/EC leaves in principle only a limited margin of discretion.[30]

In 2012, the Commission presented a package of proposals in order to update and modernize the present EU legal framework due to the challenges of new technologies and globalization. The package of proposals offered by the Commission in January 2012 contained two main documents: a proposal for a General Data Protection Regulation to replace the current Directive 95/46/EC and a proposal for a Directive to replace the current Council Framework Decision 2008/977/JHA for the area of criminal law enforcement. As a final result of the reforming steps targeting some imaginative

[29] Irene Kamara & Paul De Hert, *Understanding the balancing act behind the legitimate interest of the controller ground: A pragmatic approach,*4, (Aug, 2018).

[30] NADEZHDA PURTOVA, PROPERTY RIGHTS IN PERSONAL DATA A EUROPEAN PERPSECTIVE 162, (2012).

innovation to ensure a more effective protection, the General Data Protection Regulation was proposed in a way that suits the needs and the perspective of the time which will be further detailed specifically compared with the Directive in the next chapters.

2.2 Conscious Choice of the Legal Instrument

Lynskey notes that EU data protection regime have key characteristics which distinguishes it from other regimes in the world. [31] Firstly, EU regime is categorized an omnibus regime while a sectoral regime places in United States. In EU, the data protection rules apply to both public and private actors regardless of the sector by independent supervisory authorities. Second characteristic of EU regime consists of the most relevant one to the subject of this thesis: legitimizing regime. If the data processing has a legal basis and complies with the established protections, then such data processing is in principle legitimate. Rights-based regime and extra-territorial application constitute other features of the EU data protection regime.[32]

The criteria for legitimate processing in both the Directive and the Regulation are quite similar. There is a common misinterpretation that express consent can be used as the rule in data processing and other legal bases can be used as an exception to this rule, whereas there is no hierarchy between legal bases in either the Directive or the Regulation. Instead, the data controllers can use any of the legal grounds determined in order to legitimize the data processing. Article 7(f) of the Directive and Article 6/1/(f) of the Regulation enumerate legitimate interest as one of the other legal grounds to legitimatize data processing in a similar manner, however the change of the legal instrument and of the regulation method have paved the way for great differences in terms of the effect of the two regulations on data protection law, although they describe the same subject in terms of content.

[31] LYNSKEY, supra note 6.
[32] Id.

Unquestionably, Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data enacted on 24 October 1995 constitutes one of the most effective regulations in data protection law. Although the Directive is also based on the right to privacy, such as the Council of Europe and United Nations Regulations, as described above, a different window has been opened by the fact that this right has been included distinctly in the Charter of Fundamental Rights of the European Union. The Directive not only sets out the basic concepts and principles in this area similar to previous regulations, but also for the first time it mandates that an authority be responsible to monitor effective protection and that each Member State create a supervisory authority to monitor implementation.

Moreover, Article 29 Working Group has been the most important value that Directive has added to the world of personal data, since in addition to its role in advising Member states and the European Commission, the Working Group aims to bring different government practices to uniformity.[33] Despite the contribution of the Directive to the data protection law, it could not be escaped from the need for wide ranging review facing the world where information technology is playing a prominent role in both public and private fields. Since the extensive monitoring of consumer behavior and providing 'free' services in exchange for monitoring has created paved the way for uncontrolled using of data, in Hustinx's words, "the review of the EU legal framework for data protection has taken place in a context where both the need for more effective protection and the challenges to deliver that protection in practice have increased enormously."[34]

The Directive lit the first spark for the European Union's stance in this area and its returns were quite critical, however it was time to take a new step with the undeniable impact of globalization in this period when the law had great difficulties in capturing technology. The two Eurobarometer surveys namely Special Eurobarometer 196[35] surveying European citizens' views and Flash Eurobarometer 147 focusing on the

[33] HÜSEYİN MURAT DEVELİOĞLU, 6698 SAYILI KIŞISEL VERILERIN KORUNMASI KANUNU ILE KARŞILAŞTIRMALI OLARAK AVRUPA BIRLIĞI GENEL VERI KORUMA TÜZÜĞÜ UYARINCA KIŞISEL VERILERIN KORUNMASI HUKUKU 44, (2017).

[34] Hustinx, supra note 5, at 2.

[35] https://data.europa.eu/data/datasets/s325_60_0_ebs196?locale=en.

views of businesses published in 2003[36] by Internal Market Directorate demonstrate that if privacy matters it should be concerned about effectiveness of legal guarantees and requirements and substantial discrepancies among Member States concerning data protection.[37] The Communication by the Commission in 2010 namely "A comprehensive approach on personal data protection in the European Union" aimed at directing from the same point of view, stressing that the protection of the fundamental right to data protection and the free flow of personal data consist of two permanent goals of the European Union integration and also the Directive. Witnessing the diversity and complexity in respect of application of the Directive among Member States which cause loss of effectiveness, it was underlined that new challenges on the data protection law require the European Union to develop "a comprehensive and coherent approach" which resulted in intense work to prepare the General Data Protection Regulation with hundred pages including 99 Articles and 173 Recitals.

As stated in the Opinion of the European Data Protection Supervisor on the data protection reform package, The EDPS regrets that the Commission has chosen Directive which constitutes a self-standing legal instrument in EU law since its level of protection is inadequate and by far inferior to the Regulation.[38] In her speech in 2012 Viviane Reding, Vice President of the European Commission and Member of the EU Justice Commission, affirms that the Regulation shall unleash the potential of digital single market and save businesses around 2.3 billion euros per year simplifying the regulatory environment and overcoming bureaucratic hurdles.[39] It can be concluded that one of the reasons behind the success of the GDPR originates in the correct choice of the legal instrument. Therefore, before mentioning main lines of the Regulation in detail compared to the Directive in the context of legitimate interest, it would be appropriate to briefly explain the hierarchy of norms in European law.

[36] https://search.gesis.org/research_data/ZA4157

[37] Yves Poullet, *The Directive 95/46/EC: Ten years after,* 22*,* Computer Law & Security Report, 206-217, (2006).

[38] Opinion of the European Data Protection Supervisor on the data protection reform package, (March 7, 2012), https://edps.europa.eu/sites/edp/files/publication/12-03-07_edps_reform_package_en.pdf.

[39] Viviane Reding, The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the. Munich: Innovation Conference Digital, Life, Design Munich (Jan 22, 2012). https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_12_26.

Article 288 of the of the TFEU lists the acts which can be adopted by the European Union to exercise its competences. European law is structured on two legislations namely primary and secondary legislation accordingly. While EU Treaties, constitutions, the Charter of Fundamental Rights and general principles established by the CJEU constitute the primary legislation, all the EU acts adopted by the EU institutions, such as regulations, directives and decisions derived from the principles and objectives set out in the treaties compose the elements of the secondary legislation. As enshrined in the *Van Gend & Loos* judgment of the CJEU, the fact that individuals may directly invoke their rights before national and European courts regardless of whether a judicial remedy under national law exists consists one of the key points of EU law.[40] The direct effect has two aspects which are horizontal and vertical direct effect. While an individual invoking a provision of EU law in relation to another individual results in horizontal direct effect, an individual invokes a provision of EU law in relation to the state, vertical direct effect comes to the stage.[41]

Under this categorization, regulations have direct effect since they are "binding in its entirety and directly applicable in all Member States" as stated in Article 288. As to the directives, since they are acts addressed to Member States which must be transposed into national law and Member States have margin of discretion implementing the provision, they do not have direct effect in principle. While the directives bind each Member State addressed in terms of the required outcome, it leaves the choice of form and method to the national authorities. However, in situations where its provisions are unconditional and sufficiently clear and precise it is accepted the Directive has vertical direct effect to protect the rights of individuals.[42]

The growing gap between data protection in the first pillar (internal market) and the third pillar (enforcement and judicial co-operation) which derives from the special nature of European law constitutes one of the main challenges on the subject.[43] EDPS states in its Opinion *"it would be highly preferable to wait for the harmonization of the*

[40] Case T-26/62, NV Algemene Transport- en Expeditie Onderneming van Gend & Loos v Netherlands Inland Revenue Administration, 1963 E.C.R. 00003.
[41] ROBERT ALEXY, THE OXFORD HANDBOOK OF COMPARATIVE CONSTITUTIONAL LAW, (Michel Rosenfeld & Andras Sajo eds. 2012).
[42] Case T-41/74, Yvonne van Duyn v Home Office, 1974 E.C.R. 01337.
[43] PURTOVA, supra note 30, at 189.

pillars under EU law".[44] The Directive provided a framework mostly at national level authorizing national data protection commissioners to monitor Member States and allowing prosecutions only at national level. Therefore, it should be noted that the name of the GDPR instead of a directive is a very valuable step within the framework of personal data law. Although the Directive was considered a preferable solution leaving space for implementation to Member States, in the data protection field, it was needed to regulate the vast majority of data processing activities with a Regulation which should be seen as a turning point signaling the shift from a local phenomenon to an EU concern aiming a forced exit of this particular field of law from Member State level to EU level.[45]As a reflection of the 95/46/EC directive, a uniform application has not been reached in the field of personal data, as it is seen that 28 Member States have accepted 28 applications that comply with the basic principles of the directive but show differences. However, ensuring the same protection for personal data throughout the EU should be considered an important part of the digital common market strategy of the EU. The change of the legal instrument is considered a lead to a further "Europeanization" of data protection law, due to the fact that it shall eliminate, in theory, the discretion of incorporating the legislation in their national law system. The cooperation between DPAs and increasing volume of jurisprudence by CJEU under GDPR shall enhance the integration of national data protection systems.[46] Consequently, it is an appreciable development that this field is regulated not by a directive, but by a regulation that is directly applicable in every Member State and came into in force in 2018 suppressing the enforcement of the Directive[47].

In conclusion, although significant literal differences between the provisions of the Directive and the Regulation on legitimate interest, the negative effects of the lack of legal certainty, which will be examined in the next chapter, of the concept of legitimate interest have been tried to be prevented by the amendment made in the selection of legal instruments, but it is controversial whether this effort is successful or not.

[44] Opinion of the European Data Protection Supervisor on the Final Report by the EU-US High Level Contact Group on information sharing and privacy and personal data protection (2009/C 128/01), https://edps.europa.eu/sites/edp/files/publication/08-11-11_high_level_contact_group_en.pdf

[45] Paul de Hert & Vagelis Papakonstantinou, *The new General Data Protection Regulation: Still a sound system for the protection of individuals?,* 32, Computer Law & Security Review, 179-194, (2016).

[46] LYNSKEY, supra note 6, at 7.

[47] DEVELİOĞLU, supra note 33, at 44.

2.2.1 Conjunctive with Article 5, not selective

In respect of data protection law, in order for a legal ground to be used in the right place and at the proper time to examine, it is indispensable to examine the legal ground with a holistic approach, not alone, and to develop a better understanding about its complementary elements. Even though the data controller does not have to present any other measures to show that the data processing activity is lawful, it will still have to worry about the rest of the Regulation, from the principles under Article 5 – transparency, data minimization, purpose limitation etc., to the rights of the data subject, the accountability provisions on data protection officers, registers of processing activities, data protection impact assessments, security requirements and so on.[48]

The general principles relating to processing of personal data are listed in the Article 5 of the Regulation parallel with the Article 6 under the Directive. These principles are such principles that they constitute the prerequisite of data protection law that all data processing activities must be complied with, even if there is consent of the data subject listed in the Article 6, any breach of the principles here will render the entire data processing process illegal. On the other hand, Article 6 of the Regulation parallel with the Article 7 in the Directive set the criteria "for making data processing legitimate" though its provisions that the consent was introduced accompanied with other lawful grounds. In conclusion, the relationship between two articles should be described as conjunctive, not selective.[49] Likewise, in the Opinion of WP29, the Working Party emphasizes that "the consent does not negate the data controller's obligations under Article 6 with regard to fairness, necessity, and proportionality, as well as data quality."[50] In other words, no legal ground stated in Article 6 can eliminate the need to respect the principle under Article 5 of the Regulation. Purtova calls these substantive principles as "first cluster of rules" in data protection law which are the goals to be achieved creating a common value.[51]

[48] Future of Privacy Forum and Nymity innovating compliance, supra note 1.
[49] Hert & Papakonstantinou, supra note 45.
[50] Opinion 12/2011 smart metering 00671/11/EN WP 183 (Apr. 4, 2011).
https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp183_en.pdf
[51] PURTOVA, supra note 30, at 162.

In this context, legitimate interest as one of the legal grounds in data protection law can legitimize the data processing only under the circumstances of the compatibility with the general principles which are lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, and confidentiality. The detailed analysis of all principles is far beyond the subject of the thesis; yet, a general information will be provided to see the context.

Lawfulness and fairness indicate to act in accordance with the legal regulations, especially the laws, and to act in accordance not only with the written texts but also with the good faith principle. Transparency is the new data protection principle under Article 5 which does not exist in the Directive. It aims to enable the data subjects to know by whom and for what purpose their personal data is processed in any case.[52] The Regulation complements the transparency principle stating the manner of the provided information under the Article 12 and the content of the provided information under the Article 13 and 14 by the data controllers.

Under the purpose limitation principle, the purpose of the data processing activity should be notified to the data subject while the data is being collected, and the data should be processed in accordance with the purpose of collection. Furthermore, this principle does not cover only the collecting period, but it also includes further processing activities[53]. As to the data minimization principle, it means that if the data controller does not provide more data than necessary to achieve its purpose, and if the data controller evaluates whether the processing of personal data is necessary to achieve its purpose, and concludes that it is not necessary, it prefers this way first. Besides, the personal data shall accurate and kept up to date, where necessary according to the accuracy or information quality principle and stored only for necessary period under the storage limitation principle.[54] Right to erasure ("right to be forgotten") granted to the data subject under the Article 15 of the Regulation constitutes a significant reflection of the storage limitation principle.[55] Finally, using appropriate or

[52] DEVELİOĞLU, supra note 33.
[53] Opinion of the European Data Protection Supervisor, supra note 38.
[54] PURTOVA, supra note 30 at 162.
[55] European Data Protection Board, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default Guidelines, (Nov 13, 2019).

organizational measures technical for the data processing in a secure manner constitutes the integration and confidentiality principle under Article 5.

As a result, the notion of legitimate interest under Article 6 and its application should be considered as a whole with above mentioned principles.

2.2.2 Among other legal grounds of legitimate processing

In respect of data processing, it is undeniable that no legislature could predict all possible processing scenarios in future facing with massive technological developments. The key point is what the law will choose among alternative methods. Regulating in a much more restricted way which risks leaving some processing activities unregulated or ensuring to update the regulation when new processing activities emerge are seen impractical alternatives by authorities since they slow down technological and social development. Therefore, introducing general provisions like under Directive or Regulation such as consent or legitimate interest is the most preferable option comparing other alternatives.[56]

Both in the Directive and the Regulation, the legal grounds have been examined in two general categorizations, namely consent and other legal reasons. Although the impression is created in these texts that consent has a separate quality among other legal grounds, the consent does not have a superiority among legal grounds, as stated before. Depending on the nature of the concrete case, other legal reasons may be a more appropriate tool than consent for the data subject or data controller within the scope of data processing. The point where the legal grounds differ, as stated by WP29, is that the processing of consent and data is at the discretion of the data subject. On the other hand, all other legal grounds allow processing within the scope of a special legitimate interest where it is appropriate and necessary to process personal data, regardless of consent, provided that the safeguards and measures are complied with.

It is seen that the word "necessary" is used in all of the literal expressions of legal grounds other than consent in the Directive and the Regulation, therefore it can be understood that necessity test is valid for all legal grounds except the consent, whilst

[56] Wrigley, supra note 8.

the interpretation of necessity for each paragraph differs in doctrine and judicial decisions. Lynskey distinguishes between legal grounds as follows; the performance of a contract with the data subject and compliance with a legal obligation imposed on the controller allow data processing for legal reasons, while protection of the vital interests of the data subject and performance of a task carried out in the public interest allow for processing when necessary for individual or public purposes.[57] However, it is clear that subparagraph (f) of Article 6 in the Regulation, which regulates the legitimate interest, includes an additional balance test different from the others. [58] Since the separate meanings and interpretation of legal grounds are beyond the scope of this thesis, it will be focused on the interfaces of legal reasons with legitimate interests and the elements that affect each other.

Article 6/1/ (b) of the Regulation covers not only the performance of the contract to which the data subject is party, but it also covers the processing prior to entering into a contract. Since the critical point in the interpretation of the provision is to determine the data processing activity required for the performance of a contract, it is necessary to decide on the exact rationale, substance, or fundamental objective of the contract according to the WP29. While obtaining the address information of the customer within the framework of a contract signed for the delivery of a particular good can be considered within the scope of this paragraph, the creation of a profile from the preferences of this customer cannot be turned into a legitimate data processing activity for this legal reason. It is inevitable to detect that there is a tight connection with the above-mentioned purpose limitation principle while performing the requirement analysis at this point. However, as stated in the 47. Recital of the Regulation, when the processing of personal data which may include monitoring and profiling customers is strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the data controller concerned. The notions of profiling and prevention of fraud and their intersections with legitimate interest will be analyzed in detail in the Chapter 7.

As another example, although the activity of creating a database consisting of the name, surname, address, and contact information of the employees is not seen as the

[57] LYNSKEY, supra note 6, at 31-34.
[58] OPINION, supra note 21, at 13.

performance of the contract, it can be considered under the Article 6/1/(f) as the legitimate interest of the employer, who is the data controller, provided that necessary measures such as consulting the representatives of the employees are taken. Electronic monitoring of employee internet, email or telephone use, or video-surveillance of employees are mostly considered likely to go beyond the necessity element for the performance of the contract depending on the specific conditions of the case. WP29 underlines that the condition of being necessary for the performance of the contract cannot be used for contractual disputes. As a matter of course, processing of name and address information for the collection of a debt or initiating legal proceedings in case of default will not automatically make the data processing activity illegal. Instead, if the data controller has a legitimate interest in seeking remedies to ensure that his contractual rights are respected, then this case would fall into the Article 6/1/(f).

As to the pre-contractual relations, while receiving the name and contact information within the scope of sending a good or service offer upon the request of the data subject can be included in the scope of the subparagraph b, the case of providing health insurance by an insurance company by processing the medical data of its potential customer falls into the scope of the subparagraph f.

The compliance with a legal obligation of the data controller, which is specified as one of the legal grounds, consists of processing the data necessary for the implementation of an obligation imposed by law, regardless of the public or private sector. In this context, what is meant by legal obligation is not only the existence of a formal law, but also the provision of a legally valid and binding obligation which must comply with general principles of data protection law such as necessity, proportionality and purpose limitation.[59] In CJEU's case law, narrow interpretation of "law" in context of data protection was avoided in *Schecke ,* a limitation placed by a Council Regulation must be considered as provided by law. However, it should not be forgotten that it was argued that it cannot be talk about the adequacy of a legal basis without legal certainty.[60]

[59] Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector 536/14/EN WP 211 (Feb. 27, 2014). https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp183_en.pdf

[60] Case C-70/10, Scarlet Extended, 2011 E.C.R. I-11959, opinion of Advocate General Cruz Villalon at 67.

In order for clause c to be applicable, a clear and specific provision must stipulate the obligation, therefore the data controller should not have any right to choose or margin of discretion to comply with it as stated in the WP29's Opinion. The legal obligation criterion does not exclude legal systems where the law only sets a general purpose, and the obligations are established by secondary regulations or binding decisions. On the other hand, in cases where the regulatory authority only determines general policies and conditions and carries out data processing activities by using its executive power, it is necessary to analyze the conditions of legitimate interest under the Article 6/1/(f) rather than Article 6/1/(c).[61]

The wording of "vital interest" in the Article 6/1/(d) evidently demonstrates that this provision has a limited application. When evaluated together with the Article 9/2/(c) which limits the use of this ground to cases in which consent cannot be used as a legal ground, a restrictive interpretation must be given to this provision according to the WP29. In order to be able to rely on this legal basis, it is generally accepted that life and death situations must be experienced, and it comes into play when it comes to personal data containing health information.[62]

The legal ground of public task regulated under the Article 6/1/(d) relevant to the public and private sector covers both the cases where the data controller itself has an official authority and the data controller does not have such authority but is requested by a third party having such authority to disclose personal data. To guarantee legal certainty, the official authority or public task should be given by the statutory laws or other legal regulations. The situations where the professional associations to carry out disciplinary processes regarding their members by using their official authorities or a municipal authority running a local swimming pool fall into the scope of this legal ground. When the data controller is requested by a public authority competent to cooperate with a criminal investigation, the data processing realized by the data controller can be considered in the exercise of official authority vested in the controller. In *Worten* case (Worten – Equipamentos para o Lar SA, 2013), the fulfillment of the

[61] OPINION, supra note 21, at 20.

[62] Information Commissioner's Office, Guide to the General Data Protection Regulation Lawful Basis for Processing Vital Interests, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/vital-interests/.

necessity criterion is linked with the contribution to the more effective application of the legislation interpreting widely and the obligation of the immediate access of the national authority to the record of working time is considered necessary.[63] WP29 underlines that public task ground and legitimate interest have common features in terms of additional safeguards and measures and the right to object foreseen under the Article 14 of the Directive in parallel with the Article 21 of the Regulation. Hence, the two legal grounds would be interchangeable if the following sentence was not included in the GDPR, unlike the directive: *"Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks."* In this case, although the GDPR separated the application areas of the two legal grounds, with a narrow interpretation it might be arguable that processing for proper management and functioning of the public authorities could still be possible under the legitimate interest ground according to the WP29's Opinion.

2.2.3 Relationship with special categories of personal data

Special categories of personal data are defined, by their nature, particularly sensitive data in respect of fundamental rights and freedoms requiring specific protection as the risk of their processing is significant concerning fundamental rights and freedoms, therefore in principle such personal data should not be processed, unless processing is allowed under the conditions set out in the Regulation. The special categories of personal data under the Article 9 of the Regulation with a separate heading indicates that its interpretation and application require special attention. It is an undeniable fact that the Article aims at a much higher threshold of protection for certain specially determined personal data.

When Article 9 is examined, although the legitimate interest is not envisaged as a general exception in the processing of sensitive personal data, it is possible to see the elements of legitimate interest under Article 9/2. Legitimate activities by a non-for-profit body ground and establishment, exercise or defense of legal claims are the grounds which are closely linked to the legitimate interest clause.

[63] Case C-342/12, Worten — Equipamentos para o Lar SA v Autoridade para as Condições de Trabalho, 2013 E.C.R.

Given the reassembling conditions with the Article 6, it raises the question of whether there is an inclusive or exclusionary relationship between Article 6 and Article 9. On the one hand, if Article 9 is designed as *lex specialis*, it can be considered that special categories of personal data can be processed without complying with Article 6, on the other hand these articles should be handled in a cumulative way as explained in WP29's Opinion.[64] However, 51. Recital of the Regulation makes it clear from which point of view it should be approached affirming that the specific requirements under Article 9 does not exclude the general principles and the conditions for lawful processing. WP29 emphasizes that considering that Article 9 already brings exceptions to the prohibition and only limits the scope of the prohibition, it cannot be considered sufficient for data processing on its own. Consequently, Article 6 and Article 9 must be applied, where appropriate, cumulatively.

Although rare cases where sensitive personal data can be processed on the basis of legitimate interest, in cases where biometric entrance system is used in scientific research laboratory working with lethal viruses, legitimate interest ground may be applicable. Due to the high risk to public health if these viruses were to escape the premises, provided that appropriate measures are taken to reduce the misuse. For instance, the fact that biometric data is stored on personal employee cards and not in a centralized system is considered an appropriate practice in the WP29's opinion.[65]

2.2.4 Other related articles

Legitimate interest is a concept included not only in the article listing the legal grounds for data processing, but also in various provisions of the GDPR, therefore the other related articles of legitimate interest should also be examined in order to develop a better understanding of its context.

Article 13 and Article 14 which regulate the procedure and principles in the scope of information to be provided where personal data are collected from the data subject and where personal data have not been obtained from the data subject mention also the legitimate interest listing the required information to provide the data subject. The fact

[64] THE EU GENERAL DATA PROTECTION REGULATION (GDPR) A COMMENTARY 309-345, (Kuner et al. eds, 2020).
[65] OPINION, supra note 21, at 64.

that it is regulated under the GDPR with a separate clause that the data subject should be informed about the legitimate interests pursued by the data controller or the third party in case the data is processed based on legitimate interest should be seen as an emphasis on the fact that the legitimate interest is a general and difficult to embody concept does not constitute an obstacle to informing the data subject properly.

In terms of the rights of the data subject, all rights are entirely applicable to data processing activities based on legitimate interest with one exception namely the right to data portability. It should be underlined that, although there is no significant distinction made in terms of the rights granted to the data subject such as right to access by the data subject, right to rectification, right to erasure or right to restriction, Article 21 has an important meaning within the scope of legitimate interests. The right to object under the Article 21, which is specific to the legal reasons regulated in clauses e and f of Article 6, gives the person the right to object to the processing of his/her personal data for reasons arising from his concrete situation. As will be examined in detail in the next chapters, an exception has been made for data processing for direct marketing purposes, and it has been regulated that if the right to object is exercised, the data controller cannot rely on the aforementioned reasons and cannot continue the data processing under any circumstances. In the WP29's Opinion, the right to object should be seen as a complementary factor rather than contradictory factor of the balancing test under legitimate interest clause. At this point, it is necessary to draw attention to the difference in the Directive and the Regulation on the subject, since the party who must show the compelling legitimate interest in order to have this right in the Directive is the data subject, while in the GDPR this is replaced by the data controller. In the current situation, the data subject has this right in any case unless the data controller demonstrates that the processing has legal grounds that override the interests, rights, and freedoms of the data subject or that it is necessary for the establishment, exercise, or protection of a right, otherwise the data cannot continue to be processed.

The right to data portability under Article 20 of GDPR, the exception mentioned above, is the only right of the data subject that does not apply to processing based on legitimate interest which only applies where the processing is based on consent or a contract. It allows individuals "to obtain and reuse their personal data for their own purposes across different services" and "move, copy, or transfer personal data easily

from one IT environment to another in a safe and secure way, without hindrance to usability."[66] Some argue that the right to data portability does not constitute a new right per se, since if the consent and its withdrawal would exercise effectively, it would have presumably brought the same result. However, it can be considered as a case-specific guidance for data controllers and data subjects affecting the internet social networks market. Once the relevant industry players encourage their users to create and deepen their profiles, there is no easy way for these users to extract their information and upload it to another controller. Indeed, the Regulation addresses the problem of lack of system interoperability among internet social networks regulating this right which gives freedom to users to chance their personal data from a controller to another controller.[67] Although it is not applicable under legitimate interest clause, WP29 interprets that the recognition of the right to data portability by the data controller may shift the scales in favor of the data controller in the legitimate interest balance test, since accessing, modifying, deleting, transferring or further processing of their own data will empower data subjects and allow them benefit more from digital services. It can also contribute to the competition and consumer protection in addition to the data protection law given that it encourages service providers to provide value-added services and frees customers to switch between these providers.

It should be also noted that there is no legal reason discrimination in the obligations of the data controller and the appropriate measures to be taken by the data controller under the Regulation. Hence, taking the appropriate measures and even additional safeguards to the determined minimum thresholds under the GDPR is a significant factor in relying on the legitimate interest ground. However, since in the context of legitimate interest a specific balance test is needed to analyze whether data controller's legitimate interests are overridden by the interests or fundamental rights and freedoms of the data subject, when it is based on the legitimate interest, data processing should be subject to additional safeguards and measures to adequately protect these interests or rights and freedoms of data subjects. The effect of the

[66] Information Commissioner's Office, *Right to Data Portability,* https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-data-portability/.

[67] Hert, supra note 45.

aforementioned measures on the assessment of legitimate interests through case studies on the subject will be discussed in the following chapters.

The chapter titled "Transfers of personal data to third countries or international organizations." under GDPR is one of the sections that should be read together with the legitimate interest clause. In the Regulation, the transfer of personal data abroad is possible in cases where there is an adequacy decision of the EU Commission, appropriate measures are taken by the data controller or data processor, or there are derogations for specific conditions under Article 49. In order for the transfer to be carried out, the following conditions must be fulfilled together: If it is a non-recurring data processing activity, the transfer concerns a limited number of people, the interests, rights and freedoms of the data subject are not harmed, the transfer is necessary for the legitimate interests of the data controller, and all measures are taken by the data controller for the protection of personal data. It should be noted that a personal data transfer on the basis of legitimate interest is designed to be implemented as a last resort in the absence of adequacy decision, appropriate measures under Article 46 and binding corporate rules.

As a good example of the relationship of legitimate interest with other articles was reflected into practice through a complaint against Norwegian DPA.[68] The data subject claimed that Norwegian DPA violated several articles of GDPR processing his data on its website. Even though The General Director's replacement held that the DPA can rely on the legitimate interest ground under GDPR, it was found that the DPA violated Article 13(1)(d) because they failed to specify the legitimate interests claimed for the processing of the website feedback function and storing comments on their blog. On the other hand, Article 77 was violated since it requires data subjects to first contact the controller directly and provide documentation relating to their complaint, to the DPA. Article 5(1)(b), Article 5(2) and Article 57(2) were also analyzed, but it was found that they were not violated.

An end-to-end holistic approach is required in order to carry out a lawful data processing activity on the basis of legitimate interests. For this, before starting the data

[68] Complaint against Norwegian DPA, date of access 23.12.2022, https://gdprhub.eu/index.php?title=Datatilsynet_(Norway)_-_19/02450.

processing activity, it should be checked whether the necessary information is given to the data subject in accordance with the related articles, and whether the responsibility of all the rights of the data subject in accordance with the Regulation, in other words, the appropriate safeguards to be taken is fulfilled. It should be noted that the legitimate interest at the time the data is first processed and the legitimate interest at the time the data is transferred must be evaluated independently. In conclusion, the analysis of legitimate interest under Article 6 which regulates the lawfulness of data processing requires an assessment not in the form of an independent clause, but by reviewing all the related articles of the Regulation within the framework of personal data protection law.

Chapter 3:FACING WITH THE LACK OF LEGAL CERTAINTY

3.1 Road to EU Data Protection Reform

Lexical meaning of reform is an improvement or set of improvements made to a system, law, organization, etc. in order to make it more modern or effective.[69] It is known that reforms in history emerge when there is a need for radical change in the existing order. In this respect, two different pillars of the need for reform in EU personal data protection law came to the force at the same time, resulting in the same result. One of them was the gradual disconnection of the current Directive from today's technologies. Reding mentioned that current data protection rules were adopted in 1995 when only 1% of the EU population was familiar with the Internet, a 28.8 Kilobytes per second modem cost more than 500 euros, Amazon and eBay were still being launched, the founder of Facebook was only 11 years old and 3 years before the arrival of Google.[70] She emphasized that Just as updates are made to computers and phones, it is essential to update legal regulations.[71]

Second pillar was the problems created by the application of the Directive by Member States. In this context, perhaps the problem that should be emphasized the most is the problems experienced within the framework of legitimate interests in practice, which is the subject of this thesis. It was also stated in the first implementation report of the European Commission that the fact that legitimate interest is a concept far from predictability creates the need for further clarification.[72] Full implementation of the Directive normally requires a second step mainly consisting of reviewing other legislation that may conflict with the Directive's requirements and/or specifying certain general rules and providing appropriate safeguards besides implementing legislation. However, Member States have failed fulfilling the second stage. It was stated that national laws, which referred to the issue that detailed explanations would be made about the application of the legitimate interest clause, did not make this further

[69] Cambridge Dictionary
[70] Reding, supra note 39.
[71] Id.
[72] The Commission of the European Communities, *First report on the implementation of the Data Protection Directive (95/46/EC)*, (May 15, 2003), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52003DC0265&from=EN.

clarification. In the same report, it was stated that Clifford Chance stated that due to the provided flexibility in data processing conditions with legitimate interest ground, special attention should be given to this ground and incomplete or unclear implementations of this clause would lead to unnecessary rigidity.[73]

Even though the Directive has had several draft versions in respect of legislative stages, neither draft versions nor the final text could manage to clarify the purpose and the intent of the legislator and provide a useful guidance for its interpretation by introducing Article 7(f) of the Directive.[74] As such, the issue of how to interpret the legitimate interest has been shaped within the framework of the recommendations and opinions of national and international authorities and judicial decisions. Since the Commission led the Working Party's to contribute to achieving a more uniform application of the Directive and provide transparency in the process, WP29 published an Opinion on legitimate interest in particular.[75] In its Opinion, WP29 explains on the one hand the flexibility of legitimate interest clause has certain advantages considering that it can be applied in various cases provided that the requirements are satisfied. On the other hand, the worrying aspect of the flexibility is inconsistency among national laws and lack of legal certainty. The open-ended character of the clause may suggest a way of explaining the concept of legitimate interest with detailed and exhaustive lists. However, WP29 draws attention to the possibility that this option may lead to being misleading, unnecessary prescriptive or both.

It could be seen that problems quickly emerged with the Directive, for instance, countries behaved opportunistically to benefit from big tech with signals of weak enforcement and advantageous tax schemes. EU's attempt to address these shortfalls revealed GDPR which has serious expert consultation and deep sophistication about how information practices can be manipulated to evade regulatory goals behind it.[76] The fact that the Directive was not as effective as expected in ensuring the uniformity of the legislation on the subject led the EU institutions to work on a reform package

[73] Id.
[74] Polo Balboni et al., *Legitimate interest of the data controller New data protection paradigm: legitimacy grounded on appropriate protection,* 4, International Data Privacy Law, 244-161, (2013).
[75] OPINION, supra note 21.
[76] Chris Jay Hofnagle et al., *The European Union general data protection regulation: what it is and what it means,* Information & Communications Technology Law, 28, 65-98, (2019).

that is more compatible with the needs of the day. The history of the studies in question can be traced back to 2009, however it was necessary to wait until 2012 for the Commission to bring the reform package shaped in the GDPR center to the agenda. In addition to the GDPR, this package consisted of a directive aimed at regulating the data processing processes of law enforcement agencies. Although the European Parliament announced its support for both texts with the vote held on March 12, 2014, the final version of the reform package, which underwent some changes in 4 years with various discussions, was accepted by the European Council and the European Parliament in April 2016 and published in the Official Gazette.[77]

During preparatory works, although it was seen that the legitimate interest of the third party was excluded in the Commission's proposal in 2012, it was re-included in the final text.[78] Besides, in the Proposal, the Commission's competence to adopt delegated acts for the purpose of further specifying the conditions of legitimate interest ground for various sectors and data processing activities is not included in the Regulation provided that the interpretation of a ground should not be left to executive body such as Commission.

Another significant discussion revolved around the criticism on the Report of the Committee on Civil Liberties, Justice and Home Affairs to the European Parliament in 2012 (Albrecht Report) which provided an exhaustive list of cases when a legitimate interest of a data controller overrides the interests, fundamental rights and freedoms of the data subject.[79] However, neither the companies nor the regulators approached this restrictive solution method in a positive manner, and a general regulatory approach was displayed by not including the case list in the final text against the risk of disrupting new technological developments and business models.[80]

[77] KÜZECİ, supra note 10, at 221.

[78] The European Parliament and of The European Council, *Proposal for a Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation),* (Jan. 25, 2012), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012PC0011&from=EN.

[79] The European Parliament and of the Council Committee on Civil Liberties, Justice and Home Affairs, Draft Report on the proposal for a regularion on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), (Dec 17, 2012), https://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/pr/922/922387/922387en.pdf.

[80] Kamara & Hert, supra note 29.

Regarding legitimate interest emerged with the data protection reform, one of the most striking differences that GDPR requires careful assessment in the case of children's personal data stating in the related clause *"in particular where the data subject is a child"* which is not included in the Directive. It is obvious that the reason behind the inclusion of this phrase is the need of a higher degree of protection in cases where children's personal data is processed, since they may be less aware of the risks involved, consequences of the processing, the safeguards that could be put in place to guard against these, and the rights they have as explained in 38. Recital of the Regulation.

Article 8 titled "Conditions applicable to child's consent in relation to information society services" setting an age threshold to be offered information society services and Article 12 which requires for data controller to pay more attention on child providing transparent information are other specific articles drawing attention to children. According to the Information Commissioner's Office's Guide, the data controllers should be able to demonstrate that they have sufficiently protected the rights and fundamental freedoms of the child and that they have prioritized the child's interests over their own when this is needed considering what the child might reasonably expect the data controller to do with their personal data, in the context of the relationship with the child.[81]

As another wording difference between the Directive and the Regulation considering the legitimate interest clause, in the Directive, a third category was included namely 'A third party to whom data are disclosed'. Salom affirms this category is based on a different assumption, apart from the data controller and the data processor, and is applicable to anyone who processes data as an essentially personal activity.[82] Although telecommunications or electronic mail service, credit bureaus, list brokers and internet search engines are listed as cases in which third party to whom data are disclosed exists, the legal issues and problems that arise when trying to subject anyone who processes

[81] Information Commissioner's Office, *Children,* https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/children/

[82] Javier Aparicio Salom, *A third party to whom data are disclosed': A third group among those processing data,* 4*,* International Data Privacy Law, 177-188, (2014).

data to the legal regime applicable to data controllers and processors have been noted.[83] Consequently, it was not preferred to include this category in the text unlike the Directive.

Lastly, while Article 6/1/(f) of the Directive refers to Article 1/1, which regulates that Member States must protect the fundamental rights and freedoms of natural persons, especially the right to privacy in personal data processing, the fact that GDPR directly includes the phrase *"by the interests or fundamental rights and freedoms of the data subject which require protection of personal data"* instead of referring to this article in the GDPR shows that the substance is kept more broadly in order to protect the data subject.

Apart from these wording differences, as explained in Chapter 2, with GDPR's recitals legitimate interest ground can no longer be used as a ground for public authorities to legitimately process data in the performance of their tasks. Furthermore, the Regulation obliges data controllers to be more transparent about the legitimate interests they pursue under Recital 38, requiring that a controller must explicitly inform data subjects of their legitimate interests, document them, and remind data subjects of their right to object. When all of these are considered together, it is understood that the concept of legitimate interest is tried to be filled in order to prevent the problems experienced after the Directive, although how successful it is will be discussed in the following chapters.

3.2 Article 29 Working Party's opinion

Article 29 Working Party was established under the Article 29 of the 95/46/EC Directive in accordance with its name for the implementation and development of the Directive is tasked with overseeing the uniform implementation of the Directive by the Member States, as well as making recommendations to the Member States and the Commission in the field of personal data protection. Therefore, it was also among its duties to explain with examples how the legitimate interest would be applied and interpreted. Although EDPB has replaced WP29 with the entry into force of GDPR,

[83] Id.

WP29's established view of legitimate interest can be considered valid to the extent that it coincides with GDPR.

Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC has been a guiding light document in terms of forming the skeleton of this thesis. Apart from the intertextual differences listed above, it is useful to take the perspective of WP29 as a basis, since there are no fundamental changes in the GDPR's approach to the concept of legitimate interest. It is stated in the Opinion that the open-ended character of legitimate interest raises many important legal questions regarding its exact scope and application. Hence, WP29 follows the elimination method of what the legitimate interest clause is not by analyzing its application.

According to the Working Group, this clause cannot be considered neither as an open door nor as a last resort. Since Article 7 (f) is listed as the last option among other five legal grounds for the lawful data processing, it is criticized that it causes a wrong perception that it is seen as a legal reason to be resorted to as a last resort when other legal reasons cannot be applied to the case. It cannot be interpreted that legitimate interest "can only be used sparingly to fill in gaps for rare and unforeseen situations." The first five grounds explained above are considered a priori legitimate and there is a presumption that the balance between the different rights and interests of the data controller and the data subject is maintained. However, legitimate interest clause requires a specific test in cases out of the scope of other five grounds and any processing under legitimate interest ground has to meet the requirement of this specific balancing test. In conclusion, it should be relied on Article 7(f) regardless of other reasons, it is necessary to make an evaluation with its own requirements and features.

Another issue that has been misinterpreted regarding the legitimate interest clause is that it is preferred as an open door, considering that it has less restrictive conditions for the data controller, among other legal reasons. However, as will be explained in the following chapters, there are critical conditions for the implementation of the legitimate interest clause. Compared to other legal reasons, it is not correct to see legitimate interest as "the weakest link" in the words of WP29 or a salvation when the legitimacy of a data processing activity cannot be based on other five legal reasons. According to

the approach of the WP29, while interpreting the legitimate interest legal ground, it is necessary to consider the complementary safeguards which it offers. In terms of personal data protection law, it is important to analyze the balance correctly within the scope of legitimate interests and use it as an effective instrument at the right place and time, instead of misapplication of legal reasons such as necessity for the performance of the contract or legal obligation.

There is a fundamental reason why the above discussions are made for the legitimate interest, but not for other legal reasons. In other legal reasons, for instance when the performance of the contract or legal obligation is mentioned, these can revive common concepts in the legal world, while the legitimate interest clause may mean completely different events and situations for each legal system. In EU law, a general framework has been tried to be drawn with the rule of law and Member States have been given the freedom to act within the boundaries of this framework. As in the legitimate interest clause, legislators sometimes use this method to give space to those who enforce the regulation. With this method, on the one hand, the unpredictability of the level and impact of technology is accepted. On the other hand, in this unpredictability and endless future developments, some benchmarks are determined and rules that must be followed in any case are set. For legitimate interest, this benchmark is the condition of compliance with all general principles as well as not harming fundamental rights and freedoms. Thus, no matter what innovation talking about, it does not seem possible to go beyond these criteria.

Consequently, it should not be forgotten that the ultimate purpose of Article 7/f of the Directive is to provide the data controller with the necessary flexibility, provided that the fundamental rights and freedoms of the data subject are not undermined, as well as the necessary legal certainty and guarantees, and that such an optimum balance should be established.

Chapter 4:CRITICAL BALANCE BETWEEN DATA CONTROLLER, DATA SUBJECT AND THIRD PARTY

4.1 Existence of legitimate interest

The notion of interest is used to imply something that brings advantages to or affects someone or something in general. Legally, it means an involvement or a legal right, usually relating to a business or possessions. The interest under Article 6(1)(f) of GDPR has a similar meaning with the purpose, however it has a broader concept which can be considered in cases where a data controller may have in the processing, or the benefit that the data controller or society may obtain from processing data. While WP29 stated that an employer has an "interest" in guaranteeing the health and safety conditions of its employees, it defined the application of special access control procedures by processing personal data as his/her "purpose".

The interest under Article 6(1)(f) must be real and present, something that associates with current activities or benefits that are expected in the very near future. It must be "sufficiently clearly articulated" to allow a balancing test to be carried out against the interests and fundamental rights of the data subject. In other words, the alleged interests which are open-ended and vague, which cannot be clearly framed cannot be relied on the legitimate interest ground. Besides, it should not be forgotten that the nature of interest can manifest itself in many different ways. While the economic benefit that a company will gain as a result of analyzing the behavior of its customers with customized advertising applications to its target audience is an economic interest specific to this company, while conducting scientific research, a social interest should be discussed. Regardless of how a result will be achieved in the balance test; exercising of the right to freedom of expression or information, conventional direct marketing and other forms of marketing or advertisement, enforcement of legal claims, prevention of fraud, employee monitoring for safety or management purposes, physical security, IT and network security, processing for historical, scientific or research purposes can be cited as case studies in which it may be based on legitimate interest.

In addition to the conditions listed above for the existence of an interest, the elements of legitimacy should also be examined separately, since this interest should be legitimate. The interpretation of "existence of legitimate interest" as a first phase is made quite broader than the "balancing exercise" as a second phase. The existence of a legitimate interest does not mean that it will prevail in the balance test, therefore it should be considered only as an initial step. In the balancing exercise, a much more extensive and restrictive test awaits this legitimate interest. In SWIFT case, SWIFT is a Belgian based cooperative active in the processing of financial messages which contain personal data such as the names of the payer and payee. After the terrorist attacks of September 2001, the United States Department of the Treasury ("UST") issued subpoenas requiring SWIFT to provide access to message information held in the USA. It is undeniable that SWIFT has legitimate interest complying with the subpoenas under US law. However, considering continued processing of personal data, knowing the large scale of the UST subpoenas, lack of providence information to data subjects about processing of their personal data and insufficient control measures put in place by SWIFT, it was concluded that it cannot be relied on legitimate interest clause. Processing of data in a 'hidden, systematic, massive and long-term manner' without having specified the further incompatible purpose at the time of processing the data, and without pointing this purpose out to the users of its services overrides 'the interests or fundamental rights and freedoms of the numerous data subjects under the balancing exercise.[84] In this case, the risk of non-compliance with the subpoenas in terms of SWIFT and the risks faced by the individuals whose financial data are processed are compared and it was decided that the latter is much higher since further data processing and mirroring for an incompatible purpose could have far-reaching effects on any individual.

WP29 defines the legitimacy of an interest as being acceptable under law. However, legal admissibility should not be considered limited to the law and its subordinate regulations as explained in its Opinion on purpose limitation[85]. Legitimacy is used in the

[84] Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT) 01935/06/EN WP 128 (Nov. 22, 2006), https://www.statewatch.org/media/documents/news/2006/nov/wp128.pdf.

[85] Opinion 03/2013 on purpose limitation, 00569/13/EN WP 203 (Apr. 2, 2013), https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

broadest sense including all forms of written and common law, customs, legal principles, fundamental rights etc. Hence, if data controller can pursue his/her interest in accordance with data protection law and other laws, then his/her interest should be considered legitimate. In this respect, the wording preference of "legitimate" instead of "legal" interest is crucial. Although at first glance, the concepts of legality and legitimacy seem to be indistinguishably intertwined, when the concepts are examined in depth, there are areas where both concepts intersect, in contrast the points where they differ from each other are striking. This form of discussion has been shaped in parallel with the debate between the state of law and the state of substantive law. As Voigt points out, the problem of legality arises where there is a lack of legitimacy in the regulation and actions of authoritarian regimes such as the Nuremberg laws.[86] Although legality is accepted as an integral part of a rule of law, it is not sufficient on its own. Legitimacy serves to complete the rule of law by adding purpose and value elements.[87] Consequently legitimate interest might not be stemmed from a legal instrument, but in any case, this interest has to be in accordance with the law and not violate the law.[88]

As explained in Section 2.2.2, there are different opinions in the public sector on the basis of legitimate interests. Along with the last sentence of Article 6/1/(f) of the GDPR, the legitimate interest clause cannot be relied upon in cases where public authorities process personal data within the scope of the performance of their tasks. In the case of a narrow interpretation of the concept of performance of duty, it will be possible to assess that public authorities may have legitimate interests in matters related to management and functioning that fall outside this scope.

Finally, it is also necessary to analyze the situation of ownership of the legitimate interest to a third party other than the data controller. In this context, the relationship between the individual and the data controller is a key element in order to understand the legitimacy of the processing activity. It does not necessarily matter if there is a direct or indirect relationship between the individual and the data controller to have a legitimate interest, yet it still can be a factor to consider exercising a balancing test. One

[86] RÜDIGER VOIGT, LEGALITÄT OHNE LEGITIMITÄT: CARL SCHMITTS KATEGORIE DER LEGITIMITÄT 9-11, (2015)
[87] Mehmet Cafer Şakar, *Carl Schmıtt'te Yasallık Ve Meşruluk Üzerine Bir İnceleme*, 9, (2017).
[88] Kamara & Hert, supra note 29.

of the most common situations in the application of the legitimate interest of a third party may be the publication of data for purposes of transparency and accountability. The publication of the salaries of the top managers by the company may fall into this category due to the principle of corporate transparency, since making information available through publication is considered in the interest of other stakeholders, such as employees or journalists, or the general public, to whom the data are disclosed.[89] In the frame of the principles of personal data protection law, it is recommended to have a legal rule that clearly states and allows the content and scope of the data which are specified before to be published for the publication of personal data. Therefore, it is interpreted in WP29's Opinion that it would be more correct to rely on the ground of legal obligation in such cases.[90] However, as it will be explained in next section, even if any specific legal obligation or permission exists when the conditions of the legitimate interest clause are met and appropriate measures are provided, an open door is left.

4.2 Third Parties

The third-party issue in data protection law is a rather ambiguous issue in terms of its scope and meaning. The legitimate interest pursued by a third party which had not been included in the first text of the Directive was added with later amendments. However, the discussion based on the third parties expresses what it does not mean rather than what it means. Article 4 of the Regulation same as Article 2 of the Directive shortened the list of third parties since third parties in principle constitute a broad list specifically considering cloud computing environment. It would be problematic in terms of legitimate interest to qualify a broad category such as internet users as third parties.[91] It was aimed to emphasize that the data subject, the data controller, and any person who has an authorization for data processing with the direction of the data controller or on his/her behalf are not considered as third parties.

As it can be understood, the concept of third parties in data protection is used in a similar way in civil law. In civil law, third party means the party who is not a party to the transaction or proceeding in question. In the data protection context, any subject

[89] OPINION, supra note 21, at 27.
[90] Id.
[91] Kamara & Hert, supra note 29.

who has no specific legitimacy or authorization - which could stem, for example, from its role as controller, processor, or their employee - in processing personal data may be considered as third party.[92] To illustrate, branches of a bank would not be third parties since they are in order and instruction relationship with their headquarters in respect of processing customers' accounts. As an another example, in *Manni* case which will be further explained in detail under Chapter 5, the disclosures made through the Public Registry was deemed to be legitimized under legitimate interest ground.[93] The Court found that the interests of third parties and fair trading take precedence over the rights of individuals since the only safeguards the companies offer to third parties are their assets and the basic documents of the company should be disclosed through the Registry in order for third parties to be able to ascertain information concerning the company.

The problem in the definition explained above is that, as a rule, a third party that obtains personal data through legal or unlawful means must be a new data controller. On the other side, the use of the concept in various provisions both in Directive and Regulation demonstrates that by this way the cases where personal data might be processed by other parties which in origin were not supposed to process certain personal data are covered. WP29 gives the example of unauthorized access by an employee to explain third parties' data processing. Accordingly, an employee's access to personal data during the performance of her duty, despite no authorization given by the company, means the processing of data by a third party for the employer.

Besides the examples above; historical or other kinds of scientific research or data processing activities to combat illegal activities, such as money laundering, child grooming, or illegal file sharing online are among the examples given by WP29 in the context of legitimate interest of third parties.

4.3 Necessity element

When the wording of the Regulation text is examined, the element of necessity appears in all the subparagraphs of Article 6 from b to f. The necessity here refers to the organic

[92] Opinion 1/2010 on the concepts of "controller" and "processor" 00264/10/EN WP 169 (Feb. 16, 2010).
https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf

[93] Case C-398/15, Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v Salvatore Manni, 2017 E.C.R.

connection between the stated legitimate interest and the data processing activity. However, in the case of paragraph (f) it has a significant importance since it was aimed to prevent an inappropriate and broad interpretation of the necessity. The way to measure the fulfillment of this element is to determine whether there is an accessible method that serves the same purpose of the data controller that will allow him to obtain the legitimate interest in question, less interfering with the fundamental rights and freedoms of the data subject. In order to analyze that, it will be needed a combined and fact-based assessment of effectiveness of data processing. This means that any personal data that is not directly linked to obtaining, realizing, or otherwise accomplishing the legitimate interests pursued is not processed lawfully.[94]

Although the case-law dealing with this subject will be examined in the following chapters of the thesis, it should be said that the toolkit prepared by EDPS on the subject is a document that should be taken as a basis as a guide.[95] Since one of the purposes of this document is to consider the element of necessity, which is included in all data processing purposes of personal data law, as a separate issue, it is useful to specify the perspective of EDPS on the subject.

As mentioned in the toolkit, the case law of ECHR and CJEU which will be further examine in next chapters emphasizes that any limitations on the personal data protection requires must be applied only where the limitations are strictly necessary. Besides, it is explained that the necessity criteria shouldn't be considered as an abstract legal notion and requires a fact-based assessment due to the fact that it depends on the conditions in each case to define what strictly necessary is.

4.4 Defining interests and rights of data subject

To maintaining a balancing exercise, it is necessary to know what interests or fundamental rights and freedoms of the data subject may exist on the other scale of the balance. While only the concept of interest is used for the data controller, the use of the

[94] World Economic Forum in collaboration with Bain & Company, Inc., *Personal Data: The Emergence of a New Asset Class 5,* (Jan, 2011), https://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf

[95] The European Data Protection Supervisor, *Developing a 'toolkit' for assessing the necessity of measures that interfere with fundamental rights*, (Jun. 16, 2016), https://edps.europa.eu/sites/edp/files/publication/16-06-16_necessity_paper_for_consultation_en.pdf.

concepts of fundamental rights and freedoms in addition to the interest for the data subject implies that a broad interpretation method should be used when evaluating the interests of the data subject. The reason behind this conscious choice is the existence of an informational power imbalance between the data controller and the data subject, as mentioned in the previous chapters, and at the same time, large-scale companies and organizations can create economic benefits by deciphering the behavior profiles of individuals through big data today. By this way, the legislator has tried to minimize these negative effects experienced with this regulation and protect privacy and autonomy of individuals.

Another conscious choice in the Regulation is that the legitimacy that qualifies the interest for the data controller is not used for the data subject. Based on this, it can be concluded that individuals engaging illegal activities, for instance thefts, may have interests overriding legitimate interest of data controller such as publication of his/her picture. Therefore, as to interests of the data subjects, it should be considered in a wider scope.

4.5 Balancing exercise

The "balance" criterion is "the vaguest and most open-ended criterion" and therefore in need of explanation as stated in the Final Report of European Commission.[96] Notable differences among Member States in approach to this criterion can be observed. While in UK, the data controllers have to determine whether to process non-sensitive data on the ground of legitimate interest, in Germany it was reported that the balancing exercise was applied only in private sector. Some countries imposed more strict procedural requirements, or some set additional benchmarks using the word *"absolutely necessary"* or *"evidently prevails"* like in Greece. Under the Finnish law, the data controllers need to obtain a permit from the authority if they wish to rely on that test. Although it was tried to prevent these differences with the GDPR, it continues to be discussed whether it has been successful or not.

[96] European Commission, Comparative Study of Different Approaches to New Privacy Challenges, in Particular in the Light of Technological Developments 32, (Jan.20, 2010).

After determining legitimate interest of the data controller or a third party which is necessary for data processing and defining interests and rights of data subject, the last element that needs to be complied with is a balancing test between those interests of data controller and the interests or fundamental rights and freedoms of the data subject. On the one hand, it should be ascertained the nature and source of the legitimate interest, on the other hand the impact on the rights of the data subject should be analyzed. Comparing two sides each other constitutes the provisional balance which needs to be complemented with a final assessment if it still leaves doubt. In this case, additional safeguards applied by data controller may tip the balance on the scale.

The fact that data controller exercises his/her fundamental right enshrined in the European Charter of Fundamental Rights or ECHR such as freedom of expression and information, right of access to documents, the freedom of thought, conscience and religion or the right to an effective remedy and to a fair trial does not mean that it can be automatically relied on the legitimate interest. If exercised rights conflict with the right to privacy and the right to the protection of personal data, then it should still be analyzed whether data processing is necessary and proportionate to exercise it. The fact that the data controller acts not only on his own behalf, but also on behalf of the legitimate interests of the wider community is one of the key elements that can tip the balance in his favor in the balancing test. According to WP29, even if it is not included as an obligation in binding legal texts, if the regulatory authorities recognize or allow the data processing activity within the scope of the legitimate interest in question in their non-binding documents, it can be said that in this case there will be a weight in favor of the data controller. Even cultural or societal recognition of the interest may contribute towards a favorable assessment.

The assessment of the impact on data subject in the context of Article 6/1/(f) of GDPR should be considered as a separated analysis from the data protection impact assessment regulated under Article 35, however the assessment of impact on data subject may help identifying cases where data controller shall seek the advice of data protection authority. As explained in the Opinion of WP29, the concept of impact is a concept that should be interpreted as broadly as possible. This notion is not limited to the harm or damage suffered by the data subject, instead it covers all sorts of

actual/potential or physical/emotional impact. WP29 also emphasizes that the assessment of impact is not related to the notion of data breach, since the data subject may be affected in various ways - positively or negatively - by the processing of his/her personal data. Since the judicial decisions on which the mentioned comprehensive impact assessment is shaped will also be examined in the following chapters, it will be sufficed to identify the sources of potential impact on the data subject for now.

In order to perform the balancing test, an impact assessment is required, and one pillar of the impact analysis is risk assessment, and the other pillar is benefit assessment. Since risk analysis is a relatively familiar concept in the field of data and information security, organizations such as OWASP, NIST and ISO have already established various risk assessment criteria. However, assessing benefits and positive impact is more challenging.[97]

The likelihood that the risk materializes, and the severity of the consequences constitutes two key factors of the risk assessment. To illustrate, a risk source which has access to the Internet, exchanges of data with sites outside the EU, cannot be same with an offline source in data processing. The point to keep in mind when applying this methodology is that a purely mechanical and quantitative assessment should not be made. It is obvious that the number of affected individuals because of the data processing activity consist one of the determining factors in risk assessment. However, even if the data processing activity affects a single individual, the risk factor may be at high level. Therefore, it should be analyzed comprehensively in the risk assessment carried out within the scope of legitimate interest.

One of the first question to assess the impact on data subject is which nature personal data processing has. As explained in the Section 2.2.3, special categories of personal data under Article 9 of GDPR seeks for much higher threshold of protection comparing other categories of personal data. In general, the more sensitive the information involved, the more consequences there may be for the data subject. However, there is no blanket prohibition that special categories of personal data cannot be processed on the basis of legitimate interest, there is also no blanket permission that

[97] Kamara & Hert, supra note 29.

non-special categories of personal data can be processed on the basis of legitimate interest. In the WP29's Opinion on developments in biometric technologies, it is stated that it is possible to process biometric data on the ground of legitimate interest without obtaining consent of the data subject in cases where the security of high risk areas such as laboratories need to be specifically ensured by a mechanism that can precisely verify if the persons are entitled to access these areas since there is no alternative less interfering means appropriate for maintaining required security for this area providing that all other data protection principles are fulfilled.[98] However, in WP29's Opinion on anti-doping organizations the Working Party holds that it would be very difficult for anti-doping organizations to rely on the legitimate interest ground alone.[99] Assessing the impact on data subject, it is explained that the gravity of privacy intrusions as a result of the fight against doping by the World Anti-Doping Agency (WADA), should weigh heavily in this context. In addition, personal data which has already been publicly available continues to be being personal data, therefore further processing of personal data must be in compliance with data protection law. Nevertheless, it may be considered as a factor asserting the impact, for instance if the publication of personal data was carried out with a reasonable expectation of further use of the data for certain purposes.

Another question is in which way the personal data is being processed. Under the heading of the way a data is processed, both the width of the audience to which the personal data is transferred, and the methods used during the processing of the personal data can be considered. To illustrate, sharing it with a certain audience and sharing personal data in a public area will not have the same effect. It should also not be expected that creating more complex data sets by combining personal data in different categories by transferring personal data in its current state should have the same effect. The first scenario will be discussed further in detail under the heading of profiling and big data.

[98] Opinion 3/2012 on developments in biometric technologies 00720/12/EN WP 193 (Apr. 27, 2012), https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf.

[99] Second Opinion 4/2009 on the World Anti-Doping Agency (WADA) International Standard for the Protection of Privacy and Personal Information, on related provisions of the WADA Code and on other privacy issues in the context of the fight against doping in sport by WADA and (national) anti-doping organizations 0746/09/EN WP 162 (Apr. 6, 2009), https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp162_en.pdf.

Under GDPR's 50. Recital, the reasonable expectation of data subject is mentioned as a critical criterion to ascertain whether a purpose of further processing is compatible with the purpose for which the personal data are initially collected. However, it should also be considered as a factor to assess the impact on data subject. For instance, while the expectation of the data subject regarding the processing of health data in his relationship with a doctor or the expectation of the processing of his personal data about his private life within the scope of a divorce case with a lawyer is a reasonable expectation, the same cannot be said for a data control that does not have such a relationship with the data subject. At the time of collection of personal data, the applicable legal or contractual obligations also matter to decide whether data subject has reasonable expectation of stricter confidentiality or limitation on further use.

The status of both data controller and data subject are relevant with the impact on data subject. Big companies which have more economical and informational power in respect of its resources especially dominant actors in the market, may be very effective in convincing the data subject that they have a legitimate interest in processing their personal data. In such cases, in line with the purposes of consumer law and competition law, personal data protection law should also consider this status of the data controller in the balancing test so that the rights and interests of the data subject are not damaged. On the other hand, it is clear that the status of the data subject is also a factor to be considered. As stated above, it was stated in the legitimate interest clause under Regulation that attention should be paid to the situations where the data subject is a child. However, the situations where the status of the data subject comes into play are not limited to these cases. People who are mentally ill, asylum seeker or the elderly may need a special protection concerning data processing activities taking into account that these individuals may have difficulties in predicting the purpose and results of their data processing activities. In addition, in cases where the data subject is a worker or a student, the data controller who can establish a dominance relationship or the data controller with whom he/she is in an order-instruction relationship should also be considered exercising the balancing test.

In the light of all these explained points, it would not be realistic to expect any data processing activity to have any negative impact on the data subject. Since it is aimed to

minimize the negative effect, not its absence, it is desired to carry out a data processing activity in which an unmeasured negative effect will not occur. Not all negative effects will have the same weight on the balance. Therefore, instead of specifying a rule set on paper, the balance test should be done by considering all the circumstances of the concrete case. Wrigley developed three main arguments over the impossibility of specifying a set of rules on paper and subjectivity of balancing exercise in this respect.[100] Firstly, due to the lack of any consistent approach including case law developed by CJEU a unified methodology for identifying all of the relevant interests or weighing them up does not exist. Secondly, any attempts to create a standardized formula will probably fail, since any kind of objective test may be impossible since it is required compare two sides which will differ considerably in one case to another. This subjectivity and immeasurability cause data controllers, data protection authorities and legal advisors to create their own formulas. Lastly, the Regulation itself uses such a vague word like "overriding" which is in need of interpretation.[101] In conclusion, the ultimate goal should be to carry out this test under Regulation, which is impossible to prescribe objectively, in the most optimal way according to the conditions of the concrete case.

4.6 Additional Safeguards

There are different opinions regarding the role of additional safeguards, also known as mitigation measures, under balancing exercise. In respect of the literal interpretation, some argue that the definition of legitimate interest does not cover additional safeguards, even if legitimate interest of the data controller overrides taking these measures still must be required to protect data subject's fundamental rights and freedoms. Other such as WP29 interprets that including additional safeguards constitutes an element of the actual expected impact of the data processing and it aims to encourage the data controller to do so.[102]

[100] Wrigley, supra note 8, at 139-143.
[101] Id.
[102] Kamara & Hert, supra note 29.

WP29 distinguishes between the horizontal requirements of legitimate interest clause and additional safeguards applied by data controller. According to its Opinion, in cases where it cannot be decided which side the balance is in favor after a preliminary assessment is made according to the above-mentioned, a further assessment is indispensable to help ensure that the processing can be based on legitimate interest. At this point, additional safeguards may tip the balance. It can be said that there is a direct proportion between the impact on data subject and the importance of the additional safeguards. The more negative impact on data subject, the greater attention should be given to the additional safeguards. Although it is already certain that the data controller is obliged to take which measures in which situations as per the Regulation, there are also measures that are not clearly stated in the Regulation, but that can have an impact on the balance test if taken and may play a role tipping the balance in favor of the data controller. Working Party points to its Opinions on purpose limitation and on anonymization techniques to explain what these measures might be. Additional safeguards may include, "immediate deletion of data after use, technical and organizational measures to ensure functional separation, appropriate use of anonymization techniques, aggregation of data, and privacy-enhancing technologies but also increased transparency, accountability, and the possibility to opt-out of the processing."[103] These safeguards play a special role in reducing the undue impact on the fundamental rights and freedoms of data subjects, and thereby changing the balance to the extent that the data controller's legitimate interests will not be overridden. Indeed, legitimate interest ground seems to be the most relevant ground among other legal grounds for projects involving anonymization since W929 defines anonymization as one of the safeguards that would permit one to avoid an undue impact on the data subjects.[104] In this event, there is more likely for the legitimate interest of the controller or the third party to prevail in the balance test that is required under legitimate interest ground.[105]

[103] OPINION, supra note 21, at 31.

[104] Opinion 05/2014 on Anonymisation Techniques 0829/14/EN WP216 (Apr. 10, 2014), https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

[105] Khaled El Emam & Cecilia A´lvarez, *A critical appraisal of the Article 29 Working Party Opinion 05/2014 on data anonymization techniques*, 5, International Data Privacy Law, 73-87, (2015).

Pseudonymization techniques are also considered such measures which reduce likelihood of intervention concerning the rights of data subject.[106] Encryption with secret key, hash function and tokenization are most used pseudonymization techniques. The details of pseudonymization and encryption techniques are far beyond the scope of this thesis. It will suffice to explain in connection with the subject that pseudonymization is not a method of anonymization, instead a useful safeguard which blurs the connection of the personal data with the data subject. Encryption similarly ensures that data is less directly and less identifiable. Thus, the use of these methods by the data controller may contribute to the achievement of the result in their favor as one of the additional safeguards mentioned above.

Among the data processing principles listed in Article 5 of GDPR, accountability and transparency are the most significant principles which are closely linked to each other making pre-assessment of balance. In respect of accountability, the data controller shall be responsible and give satisfactory reasons for processing of personal data, in the meantime, provide information to the data subject in a transparent manner. In order to achieve this, the data controller first performs its own non-finalized balance assessment by defining its legitimate interest. While doing this, creating as comprehensive and detailed documentation as possible and effectively informing the data subject is seen as an example of good practice by WP29. If possible, opt-out should be provided by explaining why this processing activity will not harm their fundamental rights and freedoms in a simple language that the data subject can understand.

In this regard, it should be underlined that keeping important information from the data subject and performing data processing activities beyond reasonable expectations also touches the field of consumer law in context of unfair commercial activities. Today, the risks of free online services, especially social media, in the context of data mostly may not be noticed by users. This results in a non-transparent data processing activity. However, as stated in "The Social Dilemma documentary" – "If you are not paying the product, you are the product".[107] Therefore, accountability and transparency

[106] Opinion 05/2014 on Anonymisation Techniques, supra note 104.
[107] The Social Dilemma, (2020).

play a crucial role in respect of safeguards and overall balancing assessment. The more accountable and transparent the data processing process is, the more likely it will be to make evaluations in favor of the data controller in the balancing exercise.

According to the ICO's guidance the principle of accountability offers to the data controllers a competitive edge since it is a real opportunity to show, and prove, how the data controllers respect the data subjects' rights.[108] It also shows that the data controller actively considered the risks and put in place measures and safeguards helping to provide mitigation against any potential enforcement action. Adopting and implementing data protection policies; taking a 'data protection by design and default' approach; maintaining documentation of your processing activities; appointing a data protection officer; and adhering to relevant codes of conduct and signing up to certification schemes may be deemed to relevant measures in the context of accountability. It should be kept in mind that accountability is a living process and creating privacy management framework along with a culture of privacy in the organizations is crucial.[109]

As to the transparency, it is closely linked to the principle of fairness. Being clear, open and honest with the data subject from the start about who data controller is, and how and why personal data are processed. A transparent process comes into the stage especially where the data subjects have a choice about whether they wish to enter into a relationship with the data controllers.[110] Cookies and privacy notices appear as the reflections of this principle in practice.

To conclude, demonstrating by the data controller that he/she has acted within the framework of the principles explained above is a significant factor in obtaining a result in favor of the data controller in the balance test.

[108] Information Commissioners Office, *Accountability and Governance,* https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/

[109] Id.

[110] Information Commissioners Office, *Principle (a): Lawfulness, fairness and transparency,* https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/lawfulness-fairness-and-transparency/?q=necessary

Chapter 5:THROUGH THE EYES OF COURT OF JUSTICE OF THE EUROPEAN UNION

CJEU (hereinafter "the Court") consists one of the EU's seven institutions which incorporates two courts of law: the Court of Justice and the General Court. The Court is responsible for the jurisdiction of the European Union and ensure the correct interpretation and application of primary and secondary EU law. It reviews the legality of EU acts and decide whether Member States are complied with their obligations under EU law. One of the main roles of the Court is the unified application of EU law in Member States. It guarantees that Member States and EU institutions abide by EU law by both enforcing the law and sanctioning EU institutions as stated in the Article 251 to 281 of the TFEU.[111]

In 2009, after the Lisbon Treaty affirmed that EU Charter had the same value as EU Treaties, it was granted to the Charter legally binding force. This development redefined the EU legal architecture of fundamental rights protection creating many discussions about the role of Charter among other sources of fundamental rights protection and its provisions' interpretation. In the field of data protection, since the right of the protection of personal data does not exist in ECHR, the identification of the exact content of this right, its nature, scope and limits remained uncertain. Therefore, CJEU's case law and guidance becomes indispensable to solve the pointed confusion. However, Fuster and Gellert finds the jurisprudence of CJEU, nonetheless, in practice of limited help.[112] The Court stayed away from making references to the Article 8 of the Charter recognizing the right of the protection of personal data for a long time. In *Satamedia* case it was seen that the Court started to expressly mention that the objective of the Directive is on the one hand to permit the free flow of personal data, on the other hand to protect the fundamental rights and freedoms of natural persons in particular their right to privacy, with respect to the processing of personal data.[113] This approach continues with the *Rijkeboer* case, however the Court here defines "privacy" in a detailed way and

[111] Consolidated Version of the Treaty on the Functioning of the European Union, (2012), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012E/TXT&from=EN.

[112] Fuster & Gellert, *The fundamental right of data protection in the European Union: in search of an uncharted right,* 26, International Review of Law, Computers & Technology, 73-82, (March. 2012).

[113] Case C-73/07, Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy, 2008 E.C.R. I-09831.

incorporates many different factors of the Article 8 of the Charter, namely right of protection of personal data.[114] Advocate General Ruiz-Jarabo Colomer expressed in his opinion:

"*The fundamental right to privacy, as a general principle of Community law, found legislative expression in Directive 95/46 on the protection of individuals with regard to the processing of personal data and on the free movement of such data."*[115]

This approach demonstrates that privacy becomes synonymous with the right of protection of personal data. In *Eifert* case, the protection of personal data was mentioned as a fundamental right enshrined under Article 8 of the Charter, but it was rapidly added the close connection with the Article 7 of the Charter, namely right to privacy.[116] Thus, the Court has moved from the argument that the right of protection of personal data is an integral part of privacy to a perspective where it is a separate right, however defined only as closely related to the right to privacy.

As a result of this changing approach, the Court started to apply *modus operandi* of the right to private life to the right of protection of personal data.[117] At the end of the day, CJEU made step-by-step the proportionality test followed by ECHR making its own assessment of compliance with EU data protection law in *Rundfunk* case.[118] The fact that CJEU misplaced the proportionality requirements although it has recognized it as a separated fundamental right was found legally flawed.[119] It should not be forgotten that every regulation is built on a unique structure. The Charter contains a separate Article 52 under the heading "Scope and interpretation of rights and principles", which sets out some principles, primarily lawfulness and proportionality. However, this article also says that constitutional traditions, national law and practices should also be taken into account interpreting rights. Regardless of that, locating the conditions for the legitimacy of

[114] Case C-553/07, College van burgemeester en wethouders van Rotterdam v M. E. E. Rijkeboer, 2009 E.C.R. I-03889.
[115] Case C-553/07, College van burgemeester en wethouders van Rotterdam v M. E. E. Rijkeboer, 2009 E.C.R. I-03889, opinion of Advocate General Ruız-Jarabo Colomer at 8.
[116] Joined cases C-92/09 and C-93/09, Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen, 2010 E.C.R. I-11063.
[117] Fuster & Gellert, supra note 112.
[118] Joined cases Case C-465/00, C-138/01 and C-139/01, Rechnungshof v Österreichischer Rundfunk and Others and Christa Neukomm and Joseph Lauermann v Österreichischer Rundfunk, 2003 E.C.R. I-04989
[119] Fuster & Gellert, supra note 112.

interferences with the right to the protection of personal data in Article 8 of the Charter itself is considered inappropriate. Given the fact that the right to privacy and right to protection of personal data have diverging essence, interpreting these rights as homologous creates a misconception.[120]

In the context of EU data protection role, although there are not many cases before the Court that would impede its interpretation of the personal data protection law within the scope of the Directive or Regulation, landmark cases such as the *Digital Rights Ireland* case[121], the *Google Spain* case[122] and the *Schrems* case[123] are considered as a reflection of the Court's gatekeeper role.[124] This role on the one hand was supported by many privacy advocates, on the other hand criticized by others.[125] The main argument based on by supporters of the gatekeeper role of CJEU is that in line with the purpose of protecting a fundamental right the Court's recent case-law in respect of data protection was necessary. Kamara states three main reasons to develop this argument.[126] First, when the Directive was in force, a law dating from 1995, the obsolete data protection legislation necessitated CJEU's action. Second, existing data protection law was considered problematic causing adverse impact on fundamental rights. In this respect, Data Retention Directive 2006/24/EC, which was adopted after the terrorist attacks in Madrid, was given as an example since it did not define 'serious crime' and it did not include scalability regarding the retention periods. It imposed obligations on telecommunication operators and Internet service providers to retain certain types of data generated by individuals aiming to facilitate the work of 'competent authorities' in investigating, detecting and prosecuting serious crimes. At national level, the mentioned Directive was found unconstitutional in several jurisdictions. Third, following the constitutionalizing of the right of the protection of personal data enshrined in Article 8 of the Charter of Fundamental Rights and Article 16 of the TFEU it was upgraded to an autonomous

[120] Id.

[121] Joined Cases C-293/12 and C-594/12, Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, 2014 E.C.R.

[122] Case C-131/12, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, 2014 E.C.R.

[123] Case C-362/14, Maximillian Schrems v Data Protection Commissioner, 2015 E.C.R.

[124] Kamara & Hert, supra note 29, at 20.

[125] Irene Kamara, The Court of Justice of the EU: what to expect after the General Data Protection Regulation?, Workshop on: 'European Courts, New Technologies and Fundamental Rights' - Athens, Greece, (Jan. 2017), https://www.eliamep.gr/wp-content/uploads/2016/12/workshop.proceedings.pdf.

[126] Id.

fundamental right.[127] Thus, it can be argued that the passive role of the CJEU becomes an active role of protecting a fundamental right.

In this regard, it can be thought that it is no longer possible for the CJEU to play a role in the field of personal data protection law, when the Directive was replaced by the modern GDPR, which was regulated in the light of technological developments. However, the GDPR also has novelties such as the right to data portability, the impact assessment and data protection by design and by default which still need interpretation. Accordingly, it should be noted that since personal data protection law is faced with technological and societal challenges in its nature, even an elaborated text such as GDPR requires CJEU principles and interpretations to ensure that fundamental rights are protected.[128]

The hybrid nature of the EU personal data protection regime should be considered when examining the Court's case-law. In Chapter 2, it was demonstrated that EU data protection regime pursues both economic and fundamental rights purposes. Therefore, it should be known that relevant secondary legislation does not always carry the fundamental rights character.[129] As pointed out in *Digital Rights Ireland* case, the relationship between secondary legislation and the right to protect of personal data remains ambiguous. EU secondary legislation is interpreted sometimes in the light of the relevant right like in *Satamedia* case – Article 8 of the ECHR- and sometimes it is said to give expression to a fundamental right.[130] The discussion about the essence of the right of protection of personal data and its overlapping with the right to privacy is beyond the scope of this thesis. However, it should be underlined that the right to protect of personal data has a potential to clash with other rights such as right to freedom of information or freedom of expression and the interaction of these different right is the subject of many studies. The highest interpreter of EU law, CJEU, seems confused about the relationship of two rights relate, whether they should be relied on separately, and how each of them can be lawfully restricted. In conclusion, these inconsistencies may have negative effect on individuals.

[127] Id.
[128] Id.
[129] LYNSKEY, supra note 6, at 132-134.
[130] Id.

Another criticism of CJEU's privacy thinking approach may be developed on the base of Berlin's separation of liberties as positive and negative. In his sense, privacy can be regarded as a positive liberty. It provides benefits to an individual since it is not an absolute liberty, and some restrictions are imposed in order to lawfully limit it.[131] In contrast, the right of protection of personal data is deemed to be a negative liberty which does not empower individuals with a determinate prerogative, but instead leads the behaviors of others, as they might infringe upon this liberty.[132] This deduction is based on the idea that processing of personal data cannot be avoided in modern societies and it is never discussed whether personal data can be processed. The critical point is how this processing should be realized. Public authorities or private companies must comply with the data protection principles processing individual's data, and they can only be relied on specified legal grounds under regulations. Yet, it does not mean that data subjects are totally passive. In contrast, they are endowed with a bundle of subjective rights in order to strengthen their negative liberty and maintain some control over their personal data. Therefore, conceptual differences between these two rights should be acknowledged to make a clearer assessment in the case-law.

After a short assessment of CJEU's perspective on privacy and data protection, CJEU's case law concerning legitimate interest in data protection law will be analyzed in the next sections. As mentioned above, CJEU did not have the opportunity to interpret and apply the right to protect of personal data and naturally the notion of legitimate interest many times. Nevertheless, there are critical indicators from some cases that provide insight into how the Court interprets the balancing exercise under legitimate interest clause, as well as how it sees the criteria to lawfully use "legitimate interests" as a ground for processing. In this part of the study, the precedent-setting decisions of the Court regarding the legitimate interest will be examined.

[131] ISAIAH BERLIN, LIBERTY, (Henry Hardy ed. 2002).
[132] Fuster & Gellert, supra note 112.

5.1 Legitimate interest in national law

Within the scope of examining the legitimate interest in the light of CJEU decisions, first of all, it is necessary to draw attention to the relationship between the legitimate interest clause in the Directive and the Regulation and the national law of the Member States.

First landmark case, *ASNEF and FECEMD* is dated on 24 November 2011, long before the GDPR.[133] As explained under Chapter 2, the obligation imposed by Spanish Royal Decree on the data controller to process personal data on the legitimate interest ground only if personal data appear in public sources in the absence of consent of the data subject. One of the key findings of the Court in the judgment is that the implementing legislation of Member States cannot decide what can be considered as legitimate interest out of the scope of the Directive. Therefore, they cannot modify the grounds of data processing activity. The competency of Member States is limited to be a guideline and help to make a mere clarification of one of the data protection principles which can be considered margin of discretion. Here, Member States can adopt guidelines for the balancing exercise favoring the use of personal data available in public sources for this lawful ground to be used. However, they cannot provide additional requirements amending the scope of the legal ground of processing as a national measure. Examining the legitimate interest, the Court analyzed only two limbs of the ground answering following questions: (1) Is processing necessary for a legitimate interest? (2) Are the alleged interests overridden by the data subject's fundamental rights and freedoms?

On the first question Kamara and De Hert argue that the CJEU missed the opportunity to interpret the necessity condition of the ground.[134] In Chapter 4, the necessity condition was explained as a separate condition under legitimate interest analysis considering its significance on the subject. The question of whether there is an accessible and less interfering method that serves the same purpose of the data controller that will allow him to obtain the legitimate interest in question should be asked by the Court examining this criterion. For this, it will be needed a fact-based assessment of effectiveness of data processing. For instance, the Court could examine how it could affect data controllers if national law allowed public source data to be processed in the

[133] ASNEF and FECEMD, supra note 26.
[134] Kamara & Hert, supra note 29, at 21.

context of legitimate interest. Then, instead of such a restriction, less interfering different measures could have listed in order to show that the necessity has been exceeded, so that the legitimate interest reason does not override fundamental rights in parallel with second condition. However, in this case, the Court focused directly on balancing, passing the necessity criterion only in name instead. As to the second question, the Court did not provide further explanation on the implementation simply stating that "the seriousness of the infringement of the data subject's fundamental rights resulting from the processing" can be taken into consideration in respect of balancing exercise. The Court further noted that processing necessarily implied to be more serious if the personal data not already publicly available since "information relating to the data subject's private life will thereafter be known by the data controller and, as the case may be, by the third party or parties to whom the data are disclosed." It was underlined that opposing rights and interests concerning the balancing depends, in principle, on the individual circumstances of the particular case in question.

Breyer case is a pioneering case showing the breadth of the definition of personal data since the Court accepts the dynamic IP address as personal data if the service provider has legal means to identify the person whose data is processed with additional data that the internet service provider has. [135] However, the part of the *Breyer* decision that is significant for the subject of this thesis is that it confirmed *ASNEF and FECEMD* case[136] perspective on the lack of authority of Member States to restrict the scope of application of legitimate interest ground. The Court found a national law which did not allow that legitimate interest to be considered in data processing activity incompatible with the Directive. Under German law on telemedia, "an online media services provider may collect and use a user's personal data without his consent only to the extent necessary in order to facilitate, and charge for, the specific use of the telemedium by the user concerned, and under which the purpose of ensuring the general operability of the telemedium cannot justify use of the data beyond the end of the particular use of the telemedium." The Court interpreted national law has a more restrictive scope than that of the principle laid down in Article 7(f) of the Directive. It was emphasized that Member States cannot definitively prescribe certain categories of personal data which are excluded to be processed under legitimate interest ground such as online media user's personal data

[135] Case C-582/14, Patrick Breyer v Bundesrepublik Deutschland, 2016 E.C.R.
[136] ASNEF and FECEMD, supra note 26.

in *Breyer* decision. A case-by-case balancing test is required under the Directive to decide whether legitimate interest of website owner overrides the rights and interest of user. Lastly, collecting and using personal data with the aim to ensure operability of an online media service provider was offered as a new example of legitimate interest by the Court.

Wrigley addresses the question of the state of any valid national laws which still exist or are introduced under GDPR.[137] Although it was still a discussion matter whether the Directive has a direct effect, after the Regulation has come into force, with the effect of the legal instrument change and no longer need for the implementing legislations, these variations among Member States should no longer exist. European Commission also confirms that in its Staff Working Document after 2 years of the application of GDPR stating *"legislation in areas fully regulated by the GDPR beyond the margin for specifications or restrictions"* and explicitly referring legitimate interest legislations as one of the main issues.[138] It criticizes the self-determination of national laws of conditions for data processing activity on legitimate interest and underlines that GDPR requires each and every controller to maintain the balancing individually and benefit from legitimate interest ground. The idea behind all these explanations is that Member States are not entitled to interpret EU law. Under Article 267 of the TFEU[139] the authorization of interpreting of EU Treaties and acts of the institutions, bodies, offices or agencies of the EU is given to the CJEU. Hence, today the scope of the provisions under GDPR can only be interpreted by CJEU.

TK case is also a landmark case showing the relevance between the legitimate interest provisions in national law and the legitimate interest clause in the Directive.[140] This decision will be analyzed in further detail under the "Section 5.3 Video Surveillance", however due to its connection with the provisions in national law it was deemed appropriate to include this decision under this heading as well. The CJEU answered the question of whether Article 7(f) of Directive 95/46 to be interpreted as

[137] Wrigley, supra note 8, at 107.

[138] European Commission, Commission Staff Working Document […] Accompanying the document Communication from the Commission to the European Parliament and the Council: Data Protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation {COM(2020) 264 final},

[139] The Consolidated version of the Treaty on the Functioning of the European Union [2012] OJ C326/47 ("the TFEU"), art. 267

[140] Case C-708/18, TK v Asociaţia de Proprietari bloc M5A-ScaraA, 2019 E.C.R.

precluding provisions of national law. It was stated that Romanian national provisions authorize *"the installation of a system of video surveillance, such as the system at issue in the main proceedings, installed in the common parts of a residential building, for the purposes of pursuing legitimate interests of ensuring the safety and protection of individuals and property, without the data subject's consent."* First, the Court referred the *Breyer* case repeating "*the Member States cannot add new principles relating to the lawfulness of the processing of personal data in that article or impose additional requirements that have the effect of amending the scope of one of the six principles provided for in that article."* Second, it examined three cumulative conditions highlighting that legitimate interest condition does not require data subject's consent. After carrying out of the balancing test, the Court found that Article 7/f must be interpreted as not precluding national provisions, if the data processing activity complies with the conditions under Article 7/f of the Directive.

In conclusion, the fact that the legitimate interest clause has a flexible structure compared to other legal reasons should not be seen as a door for Member States to add and remove different elements by interpreting this clause in their own laws. While focusing on the fact that this clause is a brake for the protection of the rights and interests of the data subject, it should not be overlooked that the data controller has the right to process data based on this clause. As seen in the decisions of the CJEU, the freedom to perform a balancing test according to the conditions of the particular case is not an unlimited freedom, but a conditional freedom that cannot go beyond the criteria set in the clause. The Directive in the past, and the Regulation today, are intended to ensure that the level of protection of the rights and freedoms of individuals regarding the processing of personal data is equivalent in all Member States. Nevertheless, the approximation of the national laws applicable in this area should not be cause any decrease of the protection they afford. States must instead seek to ensure a high level of protection in the EU. In this respect, the Court does not find it correct to have additional requirements in the national law that will not allow balancing exercise according to the concrete case.[141] On the other hand, national regulations in accordance with data protection principles and legitimate interest ground are accepted following a balancing exercise.

[141] ASNEF and FECEMD case, supra note 26.

5.2 Establishment of legal claims

Analyzing of the establishment of legal claims in context of legitimate interest comes into the stage with the *Rigas* Case before CJEU.[142] In *Rigas* case, following a car accident, a trolleybus company requested a communication which contains personal data of taxi passenger in order to sue the passenger who damaged the vehicle by opening the taxi door. Yet, the national police declined to provide the identity document number and the address of the passenger. Administrative court of Latvia had doubts on the interpretation of the Article 7 (f) of the Directive and referred it for a preliminary ruling to the CJEU.

Rigas case is a useful guidance showing three cumulative conditions of legitimate interest ground explained by the Court. European Commission has also confirmed in its letter the distinction is between the different legs of the three-part test is essential since each individual requires an assessment that differs from the other parts of the test.[143] First, concerning the existence of a legitimate interest, the Court interpreted that Article 7(f) of the Directive expresses the possibility of processing data for the purposes of the legitimate interests pursued by third party rather than imposing an obligation to do so. In that regard, the Court found that the interest of a third party who needs to obtain personal information of a person who damaged their property to bring a civil action for damages can be considered as legitimate interest. Second, the Court identified a functional element of the necessity condition analyzing legitimate interest and stated that only strictly necessary derogations and limitations in relation to the protection of personal data must be applied. It includes different scales as strictly necessary and necessary considering wording. The Directive does not include the "strictly" statement, only "necessary" was used. As to the GDPR, strictly necessary is only used for the processing of personal data for the purpose of preventing fraud under 47. Recital. However, it appears that CJEU has strictly tested for both private life and protection of personal data rights.[144] The requirement of "strict necessity" arises from the significant role of the processing of personal data which entails for a series of fundamental rights, including freedom of expression. Necessity is important when it comes to the lawfulness of measures interfering in the private sphere of

[142] Case C-13/16, Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v Rīgas pašvaldības SIA "Rīgas satiksme", 2017 E.C.R.

[143] European Commission, Letter to the Dutch Data Protection Authority, (March 6, 2020), https://static.nrc.nl/2022/pdf/letter-dutch-dpa-legitimate-interest.pdf.

[144] Satamedia Case, supra note 113.

individuals.[145] Even though specific rules are adopted in respect of law enforcement such as the Directive 2016/68029,[146] this does not justify a different assessment of necessity.[147]

According to the Court, to suit a person, merely the first name and surname of the person who caused the damage does not make it possible to make that person identifiable with sufficient precision in order to be able to bring an action against him. Thus, the identification number and address information of that person are strictly necessary. Third, concerning the balancing exercise, the Court didn't make a concrete finding leaving it to the national court to decide.[148] It highlighted that an assessment should be made according to the circumstances of the concrete case. It also added the age of the data subject as a factor to take into consideration besides the seriousness of the infringement and the possibility of accessing data in public sources.

In context of establishment of legal claims, a distinction was made according to the debt collection agency's involvement by the WP29.[149] In this regard, the building company which makes the renovation of a kitchen may transfer to its lawyer to negotiate a settlement with the customer who refuses to pay the full price relying on the Article 7 (b) of the Directive. Sending a reminder to the data subject using his/her personal data falls into scope of the data processing for the performance of the contract. Although further steps taken to establish legal claims show a degree of variance as to which steps can be considered necessary for the performance of a contract, when a debt collection agency involves, it should be assessed under Article 7(f).[150] However, involvement of a third party should be analyzed carefully. Some third-party collection agents may carry out law enforcement style investigation making video surveillance or wiretapping. Here, the methods used to collect information matter. If the intrusive methods are used, the balance does not tip in favor of the data controller. Yet, if only limited checks are carried

[145] Toolkit, supra note 95, at 6.

[146] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

[147] The European Data Protection Supervisor, Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit, (Apr. 11, 2017), https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_en_0.pdf.

[148] Future of Privacy Forum and Nymity innovating compliance, supra note 1.

[149] OPINION, supra note 21, at 61.

[150] Id.

out to confirm the contact details of the data subject to start a court procedure, then data controller may rely on the legitimate interest ground.[151]

5.3 Video surveillance

Video surveillance cases is one of the cases which may concern legitimate interest issues. Audio/visual recording devices used to ensure the security of the home or office requires the examination of many factors ranging from their location, viewing distances, ways and times of recording images and sounds to the awareness of the data subjects about the recording. For instance, while a company placing hidden cameras to identify employees and visitors who smoke in unauthorized areas of the building may have a legitimate interest, since the methods that the company used disproportionate and unnecessarily intrusive comparing to the smoke detectors and visible signs, it would probably fail to meet the balancing test according to the WP29.[152]

In context of the CJEU's case law, *Rynes* case[153] addressed the issue of video surveillance from a legitimate interest perspective. Article 3 of the Directive which regulates the scope of the Directive also lists the exemptions of its application. It is stated that in cases where personal data is processed in the time of purely household activity, the Directive shall not apply. In this respect, the Court first tries to find an answer whether data processing activity of a camera system which located under the eaves of Mr. Rynes home in a fixed position and recorded the entrance to his home, the public footpath and the entrance to the house opposite constitutes the household exemption. The Court interpreted this provision in a strict manner referring the right to privacy regulated under the Charter and decided that it cannot be regarded as a purely household activity since the camera system covers a part of public space.

"...the operation of a camera system, as a result of which a video recording of people is stored on a continuous recording device such as a hard disk drive, installed by an individual on his family home for the purposes of protecting the property, health and life of the home owners, but which also monitors a public space, amounts to the

[151] Id.
[152] OPINION, supra note 21, at 64.
[153] Case C-212/13, František Ryneš v Úřad pro ochranu osobních údajů, 2014 E.C.R.

processing of data in the course of a purely personal or household activity, for the purposes of that provision."[154]

After analyzing the particular case falls into the scope of the Directive, at the next stage, the Court examined whether it could be considered within the scope of legitimate interest that Mr. Rynes recorded the suspects who had broken the window of his house in the incident and presented them in the criminal case. In this regard, the Court gives an affirmative answer stating that processing personal data with the aim of the protection of the property, health and life of his family and himself may constitute legitimate interest of the data controller. The court did not apply the three-stage test of legitimate interest and made a general assessment. However, the facts that the camera system allowed only a visual recording on a hard disk drive, as soon as it reached full capacity, the device would record over the existing recording, erasing the old material and only Mr. Rynes had direct access to the system and the data may affect the Court's decision in favor of data controller.

The Court further noted that Article 11/2, Article 13/1/d and g of the Directive should be taken into consideration in the application of the legitimate interest ground and in this particular case several exemptions to the rights of the data subject are applicable. Explaining the relationship between legitimate interest and other related articles under Chapter 2, it was emphasized that legitimate interest ground should be considered in a holistic approach in all related articles. Pursuant to the Article 11/2, in cases where the personal data is not obtained from the person himself, it is stated that the data controller does not have the obligation to inform if it is proved that it is impossible to enlighten the data subject or if it requires a disproportionate effort to enlighten the data subject. Although the Court did not express it clearly, in *Rynes* case it was implied that it was not an obligation under this article for Rynes to provide information to the passers-by regarding the camera. In addition, to prevent, investigate, detect, and prosecute criminal offences or to protect others' rights under Article 13/1/d and g, the rights of the data subjects may be restricted. The reason why the Court's approach was leading in this decision is that the interests of the data controller are co-considered in the provisions of the Directive, and it reminded the relativity the right of protection of personal data. [155]

[154] Id., at 19.
[155] Kamara & De Hert, supra note 29, at 24.

"...the application of Directive 95/46 makes it possible, where appropriate, to take into account — in accordance, in particular, with Articles 7(f), 11(2), and 13(1)(d) and (g) of that directive — legitimate interests pursued by the controller, such as the protection of the property, health and life of his family and himself, as in the case in the main proceedings."[156]

After *Rynes* case, in 2019 when the Directive was replaced by the Regulation, the Court made a decision that is considered as a guide on how video surveillance should be evaluated within the scope of legitimate interest, in which it touched on many points that it did not address in the *Rynes* decision. The *TK* case is a significant decision in that the Court examined all three conditions of legitimate interest separately and included additional explanations along with references to previous decisions.[157] TK as one of the co-owners of a building, objected the installation of three video surveillance cameras in the common parts of the building following the approving decision of the association of co-owners. One of them was installed towards the front of the building, the second one was in the ground-floor hallway and third camera was in the building's lift. TK claimed that installed video surveillance system constituted an infringement of the right to respect for private life. On the other hand, the association of co-owners stated that it was aimed to monitor people who enter and leave the building due to the fact that the lift had been vandalized on many occasions and there had been burglaries and thefts in several apartments and the common parts.

In addition, the installation of an intercom/magnetic card entry system was tried before, and it had not prevented repeat offences of the same nature being committed. While the national court asked for a preliminary ruling to the CJEU, it mainly focused on the relationship between the legitimate interest clause under Regulation and related Romanian law on the legitimate interest which authorizes personal data may be processed when the processing is required in order to protect the data subject's life, physical integrity, or health or those of a threatened third party. The main question was whether legitimate interest clause under GDPR can be interpreted as precluding national law. The

[156] Rynes Case, at 34.
[157] TK Case, supra note 140.

second aspect of the decision was whether the legitimate interest clause can be applied in particular case and its relevance with the proportionality test.

In the decision, the Court highlighted that all processing of personal data must comply, first, with the principles of data protection and secondly, with one of the legal grounds listed under Article 7 of the Directive referring *Google Spain* decision. After that, it stated three cumulative conditions of legitimate interest namely *"the pursuit of a legitimate interest by the data controller or by the third party or parties to whom the data are disclosed; the need to process personal data for the purposes of the legitimate interests pursued; and the fundamental rights and freedoms of the person concerned by the data protection do not take precedence over the legitimate interest pursued"* referring *Rigas* case. The Court emphasized that legitimate interest clause does not require the consent of the data subject.

"...It must be stated that Article 7(f) of Directive 95/46 does not require the data subject's consent. Such consent, as a condition to which the processing of personal data is made subject, appears, however, only in Article 7(a) of that directive."[158]

Deciding the existence of the data controller's legitimate interest, the Court laid out the criteria being present and effective as at the date of the data processing and not being hypothetical at that date. The Court decided that these criteria were met, based on the association's previous statements of thefts, burglaries and acts of vandalism which occurred before the installation. Then, the Court repeated the strictly necessary evaluation in the *Rigas* decision, adding a functional element to the necessity criterion of legitimate interest and stated that if an exception to the right to personal data protection is to be brought, this exception can only be accepted in a situation where it is strictly necessary. This approach of the Court does not conform to the perspective stated in the previous sections that data processing is not a prohibited activity. It is worth remembering that in today's world, where personal data is processed in every field, there are opinions that data processing is the rule, and the restriction is an exception. The Court stated that excessive data should not be processed in accordance with the data minimization principle, and it should be accepted that there is no less restrictive method left, since different methods

[158] Id., at 41

have been tried before and failed in relevant case. It further noted that the proportionality "*must be assessed by taking into account the specific methods of installing and operating that device, which must limit the effect thereof on the rights and freedoms of data subjects while ensuring the effectiveness of the video surveillance system at issue."* Therefore, the Court imposed the obligation of examining the effectiveness of the video surveillance on the data controller asking *"whether it is sufficient that the video surveillance operates only at night or outside normal working hours, and block or obscure the images taken in areas where surveillance is unnecessary."*

While the Court exercised the balancing test, it repeated the criteria such as the seriousness of infringement and the possibility of accessing data in public sources referring *Rigas* case, and it added the nature of the personal data and the nature and specific methods of processing and the reasonable expectation of the data subject on further processing data should also be taken into consideration in respect of balancing. After assessing these criteria, *"the importance, for all the co-owners of the building concerned, of the legitimate interests pursued in the instant case by the video surveillance system at issue, inasmuch as it seeks to ensure that the property, health and life of those co-owners are protected"* was balanced by the Court. In the light of the interferences of the Court, it was concluded that legitimate interest clause must be interpreted as not precluding national provisions which authorize the installation of a video surveillance system, for the purposes of pursuing legitimate interests of ensuring the safety and protection of individuals and property, without the consent of the data subjects, if the conditions laid down in Article 7(f) were fulfilled. The Court's assessment is consistent because, in the *TK* case, no criteria were added in addition to the requirements in the Directive unlike *Breyer* case. Only some of the purposes carrying out video surveillance that could be considered legitimate interests were explicitly mentioned in the national law. If the Court had looked at the regulations in an abstract way, perhaps it would have come to a different conclusion, since in national law the express and unequivocal consent is essential and the listed exceptions are not exactly the same as the Directive. However, here, when an evaluation is made according to the conditions of the concrete case, not seeking consent in a data processing activity that is considered a legitimate interest within the scope of the Directive already leads to the same result.

5.4 Economic interests

In *Manni* case, following the request of an Italian citizen who had been an administrator of a company that was declared bankrupt more than 10 years to erase his personal data from the Public Registry of Companies on the grounds that he was losing clients who checked his background in the Public Registry.[159] The national court asked the CJEU to clarify whether after a certain period of time of declaration of bankrupt, and on the request of the data subject, either erase or anonymize that personal data, or limit their disclosure.

Manni decision is significant in the sense that it accepts legitimate interest as an additional legal reason among other legal reasons namely compliance with a legal obligation and exercise of official authority and performance of a task in the public interest. The Court first acknowledged the purpose of the disclosure made by the Registry as is to protect in particular the interest of third parties joint stock companies and limited liability companies. It emphasized that checking the Registry records is the only option for third parties to ascertain information about companies and their official. While the Court decided that the data contained in the registry records only for a limited number of personal data items, namely the identity and the respective functions, it stated that it would not be possible to determine a unified time limit for the period for which these data will continue to be published from the date of dissolution of the company. Therefore, it was concluded that the persons in situation of the applicant do not have the right to obtain the erasure of personal data, as a matter of principle, after a certain period of time from the dissolution of the company. In context of right to object, in the balancing to be carried out all the circumstances in respect of the data subject's particular situation should be taken into consideration and in particular case protecting the interests of third parties and ensuring legal certainty, fair trading and thus the proper functioning of the internal market take precedence over the data subject's rights who personally chose to participate in the trading life and requested the erasure of the records. In this decision, which emphasizes that all kinds of elements can affect the balancing test and they should be considered comparatively, it is observed that an economic interest of a person, such as losing customers, is overwhelmed by the right of third parties to obtain information.

[159] Manni Case, supra note 89.

Fashion ID decision may also be considered a decision which reflects the legitimate interest approach of the CJEU, yet the Court aimed to determine which data controller has a legitimate interest rather than whether the legitimate interest conditions are met in this decision.[160] The consumer advisory center in Germany has applied to the national court about the transfer of IP address and browser information to Ireland via the Facebook like button embedded to website of an electronic commerce company called Fashion ID in Germany. The German supreme court requested for a preliminary ruling before the CJEU on the interpretation of the Directive.

In the judgment certain questions were referred concerning the relationship between national law and the Directive and the identification of the data controller(s) by the Court. However, the question on whether it can be relied on the legitimate interest ground in particular case was found irrelevant for the resolution of the dispute due to the fact that the consent of the data subjects which is required under Article 5(3) of the Directive on Privacy and Electronic Communications was not obtained.[161] Only three cumulative conditions of legitimate interest described in the *Rigas* case were referred. Due to the fact that Fashion ID is aware of the existence of the button mentioned on the website and it does not even need to have a Facebook account to transfer personal data, the Court decided that both Facebook and Fashion ID have joint responsibility and deemed to be data controllers. It was concluded that both data controllers must have a legitimate interest in order to be able to rely on the legitimate interest reason. In the light of these findings, it was stated that Fashion ID acted with an aim of being visible on social media by increasing the promotion of its products and services on Facebook, and therefore acts with economic interests and commercial purposes just like Facebook. Advocate General explained that marketing and advertising may constitute legitimate interest, however since the conditions of obtaining and transfer of personal data are not specified in this case, it is not possible to perform further analysis.[162]

[160] Case C-40/17, Fashion ID GmbH & Co.KG v Verbraucherzentrale NRW eV, 2019 E.C.R.

[161] The European Parliament and the European Council, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (July 12, 2002), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0058&from=EN.

[162] Case C-40/17, Fashion ID GmbH & Co.KG v Verbraucherzentrale NRW eV, 2019 E.C.R, opinion of Advocate General Bobek at 123.

Unlike above mentioned decisions of the CJEU, the *Google Spain* decision[163], which deals with the right to the protection of personal data as a proactive right by departing from the method of placing the right to privacy in traditional concepts, has been a turning point in many respects.[164] Mr. Costeja Gonzales, a Spanish citizen, asked both a newspaper to remove an old article about his personal bankruptcy from its online webpage and also Google to remove the link to that article from the Search Results page that appeared after entering his name in Google search engine. Pursuant rejections of both organizations the request, the applicant complaint Spanish DPA. The DPA decided that the newspaper is not under an obligation to remove the article (on the ground of journalistic exceptions granted by the Article 9 of the Directive), but it called on Google to take the necessary measures to withdraw the data from their index and to prevent access to the data in the future.

It is an unusual and unique decision in terms of evaluating the effectiveness of personal data rules, interpreting the concept of data controller, and revealing the concept of the right to be forgotten.[165] In the literature, within the scope of the decision, both the territorial scope and the material scope of the Directive has been examined. The preliminary question related to the interpretation of the territorial scope of the Directive was resolved by deciding that the Directive will be applied, and the extraterritoriality effect is given by the Court to EU data protection law. Concerning the material scope of the Directive, although Google was not the original source of data published online, since it collected, retrieved, recorded, organized, and stored data, which then disclosed to the internet users, the CJEU then held that Google must be regarded as "a controller" within the meaning of the Directive.

However, the reason for the examination of this decision under the heading of economic interests is to shed light on how the legitimate interest legal ground was applied by the Court. The CJEU delivered the judgment relying primarily on maintaining a balancing test between the rights of data subject and the legitimate interests of Google as the data controller and of internet users as third parties. In Advocate General's opinion, it

[163] Google Spain Case, supra note 122.
[164] LYNSKEY, supra note 6, at 149.
[165] Id.

was recognized that internet search engine services pursues legitimate interests in context of Article 7 (f) of the Directive, namely *"(i) making information more easily accessible for internet users; (ii) rendering dissemination of the information uploaded on the internet more effective; and (iii) enabling various information society services supplied by the internet search engine service provider that are ancillary to the search engine, such as the provision of keyword advertising."*.[166] Besides, freedom of information and freedom of expression enshrined in Article 11 of Charter and freedom to conduct a business under Article 16 of Charter were related to these three purposes in the opinion.

"…These three purposes relate respectively to three fundamentals rights protected by the Charter, namely freedom of information and freedom of expression (both in Article 11) and freedom to conduct a business (Article 16). Hence, an internet search engine service provider pursues legitimate interests, within the meaning of Article 7(f) of the Directive, when he processes data made available on the internet, including personal data."[167]

Even though the Court referred the conditions of legitimate interest ground and balancing opposing rights and interests, it did not explicitly uphold Advocate General's reasoning considering search engine services.[168]

In the judgment, one of the most remarkable points is that the Court made a difference between publishers on web pages and search engine operators in context of legitimate interest ground and held that search engine operators play decisive role disseminating personal data. They constitute more significant interference with the right to privacy while they create aggregate information, create personal profiles. These inferences have led the court to a conclusion in favor of the data subject in the balancing test. Although the CJEU as in the *ASNEF and FECEMD* case[169] stressed the dependency of the balancing test on the individual circumstances of each case, confirmed that, in principle, personal data protection prevails purely economic interests except where there is a public

[166] Joined Cases C-293/12 and C-594/12, Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, 2014 E.C.R., opinion of Advocate General Jääskinen at 95.
[167] Id., at 95.
[168] Kamara & De Hert, supra note 29, at 23.
[169] ASNEF and FECEMD, supra note 26.

interest. In this regard, the Court emphasized that the nature of the data and the publication of the data for the first time 16 years ago were also effective in making the decision.

Another point that draws attention to the methodology used by the Court in examining the legitimate interest in the decision is the assessment made together with Articles 12 and 14 of the Directive. The rights to rectification, erasure or blocking of data provided by Article 12(b) and the right to object provided by the subparagraph a of the first paragraph of Article 14 were interpreted as the rights that search engine operators must guarantee even though related personal data were published lawfully. Therefore, they must remove the data from the list of results when the data subject considers that it might be prejudicial to him/her, or he/she wishes it to be forgotten.

When these three decisions, which are examined under the heading of economic interests, are analyzed holistically in terms of the Court's approach to economic interests within the scope of legitimate interests, it is possible to say that the Court is quite cautious. Economic interest of a person faced the right of third parties to receive information in the *Manni* decision and the company's economic interest faced the public interest in the *Google Spain* decision and they were defeated in both cases. In the *Fashion ID* decision, on the other hand, although no balance test was conducted, it was seen that when it comes to the market and advertising, the Court stated that the legitimate interest review should be carried out accordingly, considering the interests of all actors together.

Many companies have built robust business models centered with personal data. Certain companies criticize personal data rules since burdensome obligations that could affect their economic interests. Therefore, the question of *"whether the economic interests of controllers and processors, or of the general public, could justify limiting the right to data protection"* arises.[170] Providing data subjects an effective control over their data is one of the key considerations of European data protection law. Especially in the digital age, an imbalance exists between the power of companies having access and processing enormous data and the power of the individuals. If there is an economic interest in the assessment of legitimate interest, it cannot be said for sure that the balancing test will be resulted in favor of the data subject or the data controller. European

[170] EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS AND COUNCIL OF EUROPE, HANDBOOK ON EUROPEAN DATA PROTECTION LAW 78, (2018).

Commission criticized the strict interpretation of Dutch DPA in the explanation note stating that pure commercial interests does not qualify as a "legitimate" interest as regards Article 6(1)(f) GDPR.[171]

"Such a strict interpretation does not allow an appropriate balance to be struck between the rights at issue, as the right to data protection is given precedence by virtue of the fact that certain interests rooted in the freedom to conduct a business are categorically considered illegitimate."[172]

As can be seen, it is not appropriate to make a categorization in this regard except for categories such as direct marketing purposes in GDPR's own recitals. This was also confirmed in the *Fashion ID* decision. Although the Court stated that both data controllers had economic interests and continued to examine other conditions of legitimate interest, in this case the Court did not end the discussion due to the nature of these interests.[173] Therefore, the Court makes a detailed assessment of who has the economic interest and responsibility in these cases, whether the rights of the data subject are respected or not, and what the protected right should be in the concrete case.

5.5 General Assessment

In this chapter, the principal decisions of the CJEU on the concept of legitimate interest have been tried to be compiled and grouped to determine the approach and point of view of the Court on certain issues. As can be seen almost all of the case law within the scope of legitimate interest, the CJEU's investigations are based on the Directive. It is not surprising that the first title relates to national law, as the Court has not yet had such an opportunity to review under the GDPR. Under 2.2. Conscious Choice of the Legal Instrument, it was explained that unlike directives, regulations apply automatically and uniformly to all the EU Member States as soon as they enter into force, without requiring a transposition into national law. Therefore, when the Directive at stake, as in *Lindqvist* stated: "*It is true that Directive 95/46 allows the Member States a margin for manoeuvre in certain areas and authorises them to maintain or introduce particular rules for specific situations as a large number of its provisions demonstrate. However, such possibilities*

[171] Letter of European Commission, supra note 143.
[172] Id.
[173] Fashion ID Case, supra note 154.

must be made use of in the manner provided for by Directive 95/46 and in accordance with its objective of maintaining a balance between the free movement of personal data and the protection of private life."[174] Therefore, the debate whether the provisions of the Directive include national law or not is inevitable. The Court did not give a generally valid positive or negative answer to this question, by examining the national legislation in the concrete case, the effects of national law on individuals were compared with the Directive. It can be concluded that it is important not to impose an additional obligation on the existing necessary conditions and not to reduce the level of protection intended to be provided for the Court to rely on the legitimate interest reason.

As demonstrated in *Rigas*[175] and *TK* case[176], the fact that CJEU managed to examine all three criteria of legitimate interest separately enabled the decisions to have the quality of guidance. The *TK* case is a pioneering case that clearly puts forward the point of view of the Court in any video surveillance case, and it is important to question whether the interest is present and effective in the examination of legitimate interests. In *Rigas*, on the other hand, the legitimate interest of third party was analyzed considering the establishment of legal claims. Besides, as mentioned under 2.2.4. Other related articles, the relationship with other related articles was confirmed in case-law associating legitimate interest clause with obligation to inform the data subject under Article 11/2 and exemptions and restrictions under Article 13.

In respect of economic interests, with the *Google Spain* case, it is seen that the Court tried to maintain its innovative perspective in the face of the huge growth of technology and examined the search engine structure. Also, it is possible to say that CJEU tends to establish the balance against commercial interests in favor of the data subject. Nonetheless, it should be kept in mind that the purpose of the GDPR is not to hamper business activities but rather to allow the conduct of business while concurrently ensuring a high level of data protection.[177] Although many questions remained unanswered in context of legitimate interest, since most of the cases are examined under the

[174] Case C-101/01, Lindqvist, 2003 E.C.R. I-12971.
[175] Rigas Case, supra note 142.
[176] TK Case, supra note 140.
[177] Letter of European Commission, supra note 143.

circumstances of the particular case rather than giving a structural guideline, the Court's help is undeniable developing doctrine on the subject.

Chapter 6:RIGHT TO RESPECT FOR PRIVATE LIFE VS. LEGITIMATE INTEREST IN EUROPEAN COURT OF HUMAN RIGHTS CASE-LAW

The best example in which the impact of disruptive development of technology on human rights has inevitably been the case law of ECtHR (hereinafter "the Court"). Over the years examining many situations related to this issue, one of the main goals of the Court was to investigate what is the fundamental right to protection of personal data. To answer this question, these core questions had also to be answered: What legal value does the protection of personal data aims to protect? Is data to be treated as a property that can be disposed of or is it an innate right granted to individuals by natural law?[178] Will we define ourselves as a buyer, seller, or individual in the data market about us?[179] Although it is important to examine the main arguments and possible consequences of existing approaches in depth, within the scope of this thesis, an analysis will be made on the basis of the view that considers the protection of personal data as a human right. However, in summary, it was useful to specify which approaches exist in the literature.

There is a strict and comprehensive regulatory regime regarding personal data in Europe. However, in the USA, sectoral solutions are preferred with a highly-market oriented approach.[180] The fact that the right to privacy, including the right to the protection of personal data, is not a constitutional right in American law, and that this right has only been discussed and accepted by jurisprudence at the end of the 19th century, are considered as the reasons behind this approach.[181] With the need to protect personal data over time, this area has been positioned within the privacy of private life. In fact, some authors have introduced the concept of informational privacy, describing the right to protect personal data as a type of privacy. Informational privacy is explained as a concept concerned with the use, transfer and processing of the personal data generated in daily life.[182] Although the debate on the degree and form of protection continues, the

[178] KÜZECİ, supra note 10, at 67.
[179] Id, at 73.
[180] Corien Prins, *Property and Privacy: Perspectives and the Commodification of our Identity,* 16, Kluwer Law International, 223-257, (2006).
[181] KÜZECİ, supra note 10, at 68.
[182] Paul M. Schwartz, *Property, Privacy and Personal Data,* Harward Law Review, 2058, (2004).

search for solid foundations in this newly developing field of protection has led to the formation of property rights and intellectual property rights theories.

One of the views put forward to protect the privacy of private life is the view that personal information is a type of property.[183] Some of the authors who support this view think that in this way, individuals can make some agreements with companies and receive financial compensation for the use of their data, or even sell them if they want, and the personal data market can function more fairly.[184] On the one hand, the property theory gives the data subject the right to demand and sue directly in case of abuse of the right, and the control over the profiles of the related persons, it is debatable how effective this control will be in today's conditions. That is to say, it is often not possible to mention that the terms of bargaining are equal between the data controllers and the data subjects. The less affluent will have to give up their data in the face of public or private companies, although this renunciation may seem voluntary, it will not.[185]

Another approach put forward by American authors is the approach that aims to protect personal data by accepting it as an intellectual property right due to its similarity with copyright. However, as Zittrain points out, important differences between the two rights need to be clarified. For example, while the danger of infringement of the protected interest about copyright is high and orderly, in the privacy of private life it is scattered and irregular.[186] On the other hand, there are also authors who oppose this approach, arguing that personal data cannot be qualified as a product of opinion.[187]

Property rights[188] or intellectual property rights theories[189] may make sense when the question of protected legal value posed above is answered only as the protection of individuals' economic interests. However, this cannot be accepted in accordance with the

[183] Lawrence Lessig, *Privacy as Property,* 69, Social Research, 247-269, (2002).

[184] Jerry Kang, *Information Privacy in Cyberspace Transactions,* Stanford Law Review, 50, 1256, (1998).

[185] KÜZECİ, supra note 10, at 70.

[186] Jonathan Zittrain, What the Publisher Can Teach the Patient: Intellectual Property and Privacy in an Era of Trusted Privication, The Berkman Center for Internet & Society at Harward Law School, (March 9, 2000). file:///C:/Users/%C4%B0rem%20MUTLU/Downloads/SSRN-id214468.pdf.

[187] KÜZECİ, supra note 10, at 72.

[188] Lessig, supra note 183; Kang, supra note 183.

[189] Pamela Samuelson, *Privacy as Intellectual Property?*, Stanford Law Review, 52, 1125-1173 (May, 2000); Corien Prins, *When personal data, behavior and virtual identities become a commodity: Would a property rights approach matter?,* Script – ed, 3(4), 270-303, (June 2006).

essence of the right. Parallel to today's dominant view, the right to protection of personal data serves a much wider area such as human dignity, individual autonomy, and the right to determine the future of information.[190]

It is not surprising that within the framework of the human rights approach, the right to protection of personal data is evaluated within the right to respect for private life at the first stage since there is a close relationship between the two rights areas. However, as it is frequently mentioned in the decisions of the ECtHR, the difficulty in defining private life naturally spread to the explanation of this relationship.[191] Therefore, as a method determined to overcome this difficulty, private life is divided into four different clusters, the public space that the person can share with everyone, the general living space, the living space that he/she can share with certain people, the private living space of the person, and the secret space, the area that the person wants to keep only to himself/herself.[192] In this context, it should be noted that data concerning sexual life, ethnicity etc. in the field of secret space is also considered as sensitive data in personal data protection law. In addition, the concept of general living space is not an area that is not worth protecting and taking audio and video recordings of CCTV systems and public areas needs to be evaluated in respect of personal data protection.

Dating back to 1890, Warren and Brandeis defined the right to privacy as the right "to be let alone" and discussed the necessity of legal protection.[193] As Westin, opinions have emerged that associate this right with personal information, and the right to privacy has been defined as the right of individuals, communities, or corporations to decide for themselves when, how and to what extent the information about them will be in contact with others.[194] Another feature of Westin is that she emphasizes the criterion of control of the individual.[195] In this definition of Westin, it is thought that the increase in the probability of individuals to relax with the developments in telecommunications in the relevant period is an important factor.[196] In a similar vein, as the need to protect personal

[190] Id., at 74-75.
[191] Niemietz v. Germany, Eur. Ct. H.R. at 29 (1992). Murray v. the United Kingdom, Eur. Ct. H.R. at 83 (1994).
[192] KÜZECİ, supra note 10, at 79.
[193] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy,* Harward Law Review, 50, 194-221, (1890).
[194] ALAN WESTIN, PRIVACY AND FREEDOM 7, 1967.
[195] Id.
[196] KÜZECİ, supra note 10, at 81.

data arises, it is a natural result that the scope of the right to privacy will be affected by current requirements and determined by associating it with personal data.

Looking at the main international documents, it is seen that Article 8 of the ECHR, adopted in 1950, only regulates the privacy of private life. As in many other issues, the ECtHR has evaluated the right to protection of personal data within the scope of the right to privacy with its decisions in the light of technological developments. Despite of the resilience of the Article 8 to technological threats, the principles of the right to privacy have been applied to areas examined within the scope of protection of personal data, such as wiretapping, file interconnection unauthorized access to personal data which were not in the minds of the drafters of the ECHR at that time.[197] The United Nations Human Rights Committee, in its general interpretation published in 1988, determined that the basic principles of the right to personal data protection should be evaluated within the framework of Article 17 of the UN International Convention on Individual and Political Rights on the protection of private life.[198] On the other hand, the Charter which is a relatively new text, the right to privacy and the protection of personal data are regulated in separate articles and it is foreseen that the regulations on the subject will be audited by an independent body.

The fact that the right to protect personal data finds its source in the right of privacy also brings some challenges. In the literature, while the right to privacy labelled "an opacity tool" and a negative right which aims to prevent State form intervening in individual's affairs and does not require any positive steps, the right to protect personal data labelled transparency tool is seen as a dynamic right which gives individuals positive rights and imposes affirmative obligations on States.[199] Therefore, the protection envisaged for the privacy of private life may mean a limited protection of the right to the protection of personal data following every movement of the data. According to the ECHR, while Article 8/1 regulates the right, it is expected to prove that the interference with this right is lawful for the reasons specified in Article 8/2. However, as explained above in the personal data protection law, the fact that the processing of data is based on a reasonable justification does not always make the storage and processing of such data

[197] Council of Europe, supra note 11, at 31.
[198] The United Nations Human Rights Committee, General Interpretation Number 16, (1988).
[199] PURTOVA, supra note 30, at 226.

lawful. Despite this distinction, there are similarities between the two rights in terms of the protected legal value.

Prosser conceived privacy tort as four wrongs and named four interests: moral integrity, honor and dignity, fame and name, material interests arising from his name and image.[200] However, Bloustein criticized Prosser's stand stating that the only interest protected by the right to privacy is human dignity.[201] Accordingly, the human dignity approach was at the forefront in the "Volkzählung" decision of the German Constitutional Court which refutes the grounds of the census law, which obliges citizens to disclose comprehensive information during the census. [202] According to the Court, at the center of the constitutional order is the dignity of the individual as a free member of society.[203]

Lynskey explained that the link between data protection and privacy can be construed in three models.[204] First model is based on the fact that data protection and privacy are complementary tools and they both serve the ultimate aim namely human dignity. Second model is construed on that data protection is a facet of the right to privacy and it was claimed that they have common denominators like family members. In third model, privacy covers the interests of personal autonomy, democratic participation, bodily integrity, family life etc., including data protection in privacy blurs the meaning of privacy.[205]

In a similar way, Paul de Hert and Serge Gutwirth emphasized non-interchangeability of privacy and data protection.[206] They explained asserting data protection law as solely or even essentially with safeguarding privacy is a misleading approach since data protection laws serve interests which are beyond traditional conceptualizations of privacy.[207] Thus, data protection cannot be covered by the scope of the protection of privacy. As a result, although the right to protect personal data finds its

[200] William Prosser, *Privacy,* California Law Review, 48, 383-423, (1960).
[201] Edward Bloustein, *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*, New York University Law Review, 39, 965, (1964).
[202] German Federal Constitutional Court, supra note 16.
[203] KÜZECİ, supra note 10, at 76.
[204] LYNSKEY, supra note 6, at 91-106.
[205] PURTOVA, supra note 30, at 225.
[206] Paul de Hert & Serge Gutwirth, *Data protection in the case law of Strasbourg and Luxemburg : constitutionalisation in action,* Vrije Universiteit Brussel From the Selected Works of Serge Gutwirth, 6, (2009).
[207] Id.

source in the right of privacy, at the end of the day, it now manifests itself as an independent right. Nevertheless, ECtHR's examination of the data protection rights within the scope of privacy is criticized, expanding the scope of the right to privacy, and reducing the importance of this right by moving away from the values that should be protected at its origin.[208]

After the tension between the right to privacy and data protection was put forward, it is beneficial to mention some general principles formed in the field of personal data protection law with the case law of the ECtHR given that based on these general principles, a further interpretation has been made on the legitimate interest by the Court. ECtHR analyzes the concept of private life in a flexible manner and avoids giving an exhaustive definition since it is a broad term.[209] The scope of the private life can include multiple aspects of the person's physical and social identity.[210] It embraces information about the person's health[211], ethnic identity[212]and elements relating to a person's right to their image[213]. The right to respect for his private and family life under Article 8 is considered the right to personal development, and the right to establish and develop relationships with other human beings and the outside world[214]

The mere storing of data relating to the private life of an individual results in an interference in respect of Article 8[215]. Determining whether the personal information retained by the authorities involves any of the private-life aspects mentioned above. Similar to the criteria considered in the balancing exercise in the decisions of the CJEU concerning legitimate interest, ECtHR also analyzes "*regard to the specific context in which the information at issue has been recorded and retained, the nature of the records, the way in which these records are used and processed and the results that may be obtained."*[216]

[208] PURTOVA, supra note 30, at 226.
[209] Pretty v. The United Kingdom, App. No. 2346/02, 2002-III Eur. Ct. H.R.
[210] Mikulić v. Croatia, App. No. 53176/99, 2002-I Eur. Ct. H.R.
[211] Z v. Finland, App. No. 22009/93, 1997-I Eur. Ct. H.R.
[212] S. and Marper v. The United Kingdom, App. Nos. 30562/04 and 30566/04, 2008 Eur. Ct. H.R.
[213] Sciacca v. Italy, App. No. 50774/99, 2005-I Eur. Ct. H.R.
[214] Burghartz v. Switzerland, App. No. 16213/90, Eur. Ct. H.R. (ser. A), (1994) and Friedl v. Austria, App. No. 15225/89, Eur. Ct. H.R. (ser. A), (1995).
[215] Leander v. Sweden, App. No. 9248/81, Eur. Ct. H.R. (ser A.), (1987).
[216] Friedl Case, supra note 214.

As it is known, the ECtHR, in the substantive examination of the decision, first looks at whether there is an interference or not, and then whether this interference is in accordance with law, whether it has a legitimate aim, and lastly it is necessary in a democratic society. In connection with the subject of the thesis, it is seen that the legitimate interest analysis is made especially under the title of necessary in a democratic society by the Court deciding whether a fair balance between legitimate interests and alleged violated rights is struck. In addition, legitimate interest is asserted by ECtHR within the framework of the principles of personal data protection law, especially the principle of proportionality.

For an interference to be considered "necessary in a democratic society" for a legitimate aim by ECtHR, it should answer a "pressing social need". Also, if the interference is proportionate to the legitimate aim pursued and if the reasons pointed out by the national authorities to justify it are "relevant and sufficient"[217]. Since national authorities should make the initial assessment in all these respects, the question of whether the interference is necessary should be answered by the Court analyzing the conformity with the requirements of the ECHR.[218] Assessing the necessity in a democratic society, in the light of margin of appreciation doctrine, the competent national authorities may have practical differences in implementing the articles of the ECHR. However, the breadth of this margin varies and depends on various factors such as the nature of the right, its importance for the individual, the nature of the interference and the object pursued by the interference. The margin will tend to be narrower where the right is crucial to the individual's effective enjoyment of intimate or key rights[219]. On the other hand, the margin will be restricted in cases where a particularly important facet of an individual's existence or identity is at stake[220].

In this chapter, ECtHR decisions concerning the relationship between the right to privacy of private life and the right to the protection of personal data will be examined within the scope of the legitimate interest. In which category of personal data the Court

[217] Coster v. the United Kingdom, App. No. 24876/94, Eur. Ct. H.R., (2001).
[218] Id.
[219] Connors v. the United Kingdom, App. No. 66746/01, Eur. Ct. H.R., (2004).
[220] Evans v. the United Kingdom, App. No. 6339/05, 2007-I Eur. Ct. H.R.

has dealt with related to the legitimate interest until today? What criteria did the Court consider when conducting a legitimate interest review? Whose legitimate interest prevailed when right to privacy encountered freedom of information? These questions will be tried to be answered in the light of the ECtHR's case law associated with the relevant literature.

6.1 *Yvonne Chave née Jullien v. France*[221]

One of the first decisions of ECtHR dealing with personal data, *Yvonne Chave née Jullien* case in 1991, is also the first bud of the Court's evaluation regarding the processing of special categories of personal data. The case concerning the recording in a psychiatric hospital file of data on the compulsory confinement of a patient was declared manifestly ill-founded and rejected by the European Commission of Human Rights. The Commission considered that the recording of information concerning mental patients serves constitutes legitimate interest not only by ensuring the efficient running of the public hospital service, but also by protecting the rights of the patients themselves. This kind of storage serves preventing the risk of arbitrary confinement and helps investigation of the administrative or judicial authorities responsible for the oversight of psychiatric institutions.[222] Yet, it should be born in mind that it will be seen how the scales shifted from the data controller to the data subject, based on the importance of special categories of personal data, in the examination of legitimate interests in the following decisions.

The applicant was confined in a psychiatric hospital following the execution of a compulsory placement by related authorities. However, after seven years the confinement was declared unlawful by the domestic courts and a compensation was awarded to the applicant. Then, the applicant asked for her name and other personal information to be removed from the central record of patients and any other record. First of all, the Government denied the existence of a central database. The patients' data was kept in a file, and it was registered by the hospital, however access to this information was only possible to the public authorities in the exercise of their powers to consult them. ECtHR was convinced by the arguments of the government on this issue stressing the files and

[221] Yvonne Chave née Jullien v. France, App. No. 14461/88, Eur. Ct. H.R., (1991).

[222] European Court of Human Rights, Guide to the Case-Law of the of the European Court of Human Rights Data protection, (Aug. 31, 2022). [hereinafter Guide]

registers contain objective and verifiable information only reachable to the persons concerned.

The Commission stated that keeping of the file and register does not constitute an interference on the grounds that this is a measure taken not against them but for their benefit. It is impossible to agree with this conclusion of the Court, since when deciding whether there is an interference or not, as a rule, it should be checked whether there is an interference with the right at stake, here right to respect for the private life. This intervention may be a measure taken by public authorities, but it cannot be decided on the premise that it is in the interest of the persons concerned. It is proven by experience that many measures taken by public authorities with this claim can cause human rights violations.

Even though ECtHR gave a negative answer to the interference question, it stated that even if there was an interference it must be regarded justified. The question of whether the interference is provided by law was not disputed in this case. The Court further specified legitimate aim pursued which are protection of health, ensuring the efficient running of the public hospital service and protecting the rights of the patients themselves, especially in cases of compulsory placement. The main point in this decision is whether the interference necessary in a democratic society. Here the Court implied the nature of data was effective affirming the information relating to the applicant's compulsory placement in a psychiatric hospital is more serious given that it caused the applicant distress since she was well-known where she had worked as a teacher. Therefore, providing adequate and effective guarantees against abuse was also considered the State's obligation pursuing its legitimate aims. Analyzing national laws which regulates above-mentioned data is no means accessible to the public, but only to exhaustively listed categories of persons from outside the institution, the Court decided that the guarantees built into the French supervision system satisfy the requirements of paragraph 2 of Article 8 of the Convention and the interference is not disproportionate to the legitimate aim pursued.

6.2 *S. and Marper v. the United Kingdom*[223]

As in *Yvonne Chave née Jullien* case, another decision that concerns special categories of personal data is the *S. and Marper* decision. Although it is a relatively old decision in terms of the date of the decision, it is one of the guiding decisions as it compares the legitimate interest of the public authority for the prevention of crime with the right to respect for private life of the data subject within the scope of Article 8. In the decision, concerning storage of personal data for the purposes of combating crime, it was concluded that "*the interests of data subjects and the community as a whole in protecting personal data, including fingerprint and DNA information, may be outweighed by the legitimate interest in the prevention of crime*."[224]

First of all, it should be noted that there are two applicants in this case, one of which is a 11-year-old. Their DNA samples and fingerprints were taken after their arrest, however the police refused both applicants' requests to destroy their personal data even though one of them was acquitted and the other's case was formally discontinued. The national court of appeal made a remarkable assessment. It listed the risks of the retention of DNA samples and stated that *"the retention of samples permits (a) the checking of the integrity and future utility of the DNA database system; (b) a reanalysis for the upgrading of DNA profiles where new technology can improve the discriminating power of the DNA matching process; (c) reanalysis and thus an ability to extract other DNA markers and thus offer benefits in terms of speed, sensitivity and cost of searches of the database; (d) further analysis in investigations of alleged miscarriages of justice; and (e) further analysis so as to be able to identify any analytical or process errors."* However, the Court of Appeal found the identified risks are outweighed by the aim of prosecuting and preventing crime. It also brought some statistical evidence about the role of retained fingerprints and samples in the detection and prosecution of crimes. It was affirmed that the fingerprints and samples which could now be retained had in the previous three years played a major role in the detection and prosecution of serious crime.

ECtHR in *S. and Marper* decision first tried to determine the place of United Kingdom among Member States by revealing some statistics from different country

[223] S. and Marper Case, supra note 212.
[224] Guide, supra note 222.

practices especially focusing on Scotland as a part of the United Kingdom itself at that time. In the light of these evidence, even though the number of Member States which allow the compulsory taking of fingerprints is steadily increasing, they do not take information in a systematic manner but in a limited way to some specific circumstances and/or to more serious crimes, notably those punishable by certain terms of imprisonment. ECtHR drew attention the fact that the United Kingdom is the only Member State expressly to permit the systematic and indefinite retention of DNA profiles and cellular samples of persons who have been acquitted or in respect of whom criminal proceedings have been discontinued.

The Court referred the Article 13 of the Directive which allows Member States to restrict certain obligations and rights provided when the restriction constitutes necessary measures to safeguard the prevention, investigation, detection, and prosecution of criminal offences. It was no doubt that all the fingerprints, DNA profiles and cellular samples constitute personal data within the meaning of the Convention 108. Although ECtHR examined separately applicants' right to respect for their private lives by the retention of their cellular samples and DNA profiles, and of their fingerprints, at the end both examinations reached the same conclusion accepting the retention of cellular samples and DNA profiles has a more important impact on private life than the retention of fingerprints.

Deciding whether an interference exists, the Court stressed the unpredictability of the rapid pace of developments in the field of genetics and information technology in respect of further use of personal data. "*Given the nature and the amount of personal information contained in cellular samples, their retention per se must be regarded as interfering with the right to respect for the private lives of the individuals concerned"* according to the Court. As to the DNA profiles, it was stated that since they may provide information about ethnic origin, they are also susceptible interfering the right to private life. The level of interference regarding these types of personal data may be different, but consequently, retention of these data constituted an interference in Court's opinion.

In the justification part, ECtHR accepted that the retention of mentioned data had a clear ground in national legislation. Yet, the Court did not find it necessary to decide whether the national law fulfills the "quality of law" requirements within the meaning of

Article 8 § 2 of the Convention given a broader issue namely necessity in a democratic society needs to be analyzed to answering whether national law provides sufficient safeguards processing data. It further notes that the retention of data was grounded on legitimate aims which are detection and prevention of crime and a broader purpose namely assisting the identification of future offenders.

Under the title of necessary in a democratic society, although prevention of crime may be accepted as a legitimate interest, it was emphasized that due to the special nature of the data, the State measure authorizing the retention and processing of data without the explicit consent of the data subject should be carefully examined by the Court.[225] ECtHR limited the scope of its analysis with the question of whether the retention of the applicants data, as persons who had been suspected, but not convicted, of certain criminal offences, was justified under Article 8 § 2 of the Convention rather than whether the retention of fingerprints, cellular samples and DNA profiles may in general be regarded as justified under ECHR.

The principles of proportionality and limited periods of storage were referred examining the case. The critical questions are whether such retention is proportionate and strikes a fair balance between the competing public and private interests. In this regard, it was underlined that great majority of Contracting States were looking for a certain gravity in the relevant crime type in order to obtain cellular samples and destroyed the DNA databases immediately or within a certain period of time after acquittal of the relevant crime. The Court interpreted that Member States setting these limits on the retention and use of data aim to maintain a proper balance with the competing interest of protecting the right to respect for private life. Thus, it came to the conclusion that the fact that a strong consensus exists among States on this subject results in narrow margin of appreciation left to the States regarding the assessment of the permissible limits. In this respect, the blanket and indiscriminate nature of the power of United Kingdom authorities on retention of data was considered a disproportionate interference since without specifying any age, time limit and the nature or seriousness of the offence of which the person was suspected fingerprints and samples may be taken. ECtHR also highlighted that in case of minor applicant the interference may be especially harmful on the grounds of their special

[225] Z v. Finland Case, supra note 211.

situation and the importance of their development and integration in society and it requires particular attention. Consequently, the interference was regarded not necessary in a democratic society by the Court.

6.3 *Węgrzynowski and Smolczewski v. Poland*[226]

Exercising of the right to freedom of expression or information under legitimate interest ground includes many different aspects which WP29 analyzed under three different practical examples.[227] First, legitimate interest ground found applicable in the case where an NGO which republishes expenses of Members of Parliament provided that the re-publication was carried out in an accurate and proportionate manner and appropriate safeguards were adopted. While making this interpretation, in terms of data controller, it has been shown that the nature of the legitimate interest is a fundamental right such as freedom of expression. The public's interest in ensuring transparency and accountability, and the data subject's expectation due to the fact that the information has been published in accordance with the law before, constitutes favorable assessment. However, WP29 warns that if expenditure information contains health data, a proactive approach should be taken to give the person the right to review their data. Although in terms of data subject, the impact of data processing was considered significant since it may lead loss of elections or a criminal investigation against him/her, on the balance data controller's interests override data subject's interests. In the second example, revealing the information about the appointment of a local councillor's daughter as a special assistant by a journalist was also seen as a case where legitimate interest ground may applicable. It was stated that one of the effective reasons here is that the data subject is a public figure, therefore his privacy in public activities is quite limited, and it was underlined that this information is in the public interest.

Third example may be the closest example to the case which will be examined below in context of the possible conflict between freedom of expression and privacy. Publishing minor criminal offences of a local amateur football player in the on-line archive of a newspaper was analyzed by WP29. The fact that even though the criminal records of the data subject are now clean, the link to this old news can be reached among the first results

[226] Węgrzynowski and Smolczewski v. Poland, App. No. 33846/07, Eur. Ct. H.R., (2013).
[227] OPINION, supra note 21, at 57.

searching his name with common search engines online was found disturbing. In this case, pursuant to data subject's request, the newspaper refused to adopt technical and organizational measures. Ensuring by data controllers that in case of a justified objection, under Article 14(a) of the Directive, the relevant part of the on-line archives will no longer accessible by external search engines or the format used to display the information will not allow search by name was considered a key role in striking a fair balance.

Węgrzynowski and Smolczewski case is notable for both examining freedom of information and right to privacy together, showing the intersections, and exercising the balance between the legitimate interest of the public in accessing information and the right to privacy of the data subject.

Before national courts, the applicants who were lawyers claimed that their rights to respect for their private life and reputation had been breached pursuant to the publication of an article which states they had made a fortune over the years by assisting in shady business deals among other politicians. Since the national courts found the allegations in the article had not a plausible factual basis and they mostly based on gossip and hearsay, the journalists were ordered to pay a certain amount of money to a charity and publish an apology. The courts noted that although the journalists had a right and obligation to inform society and enjoyed freedom of expression, they had not taken minimum necessary measures to verify the information.

Afterwards, the applicants sued again the newspaper under the same legal ground claiming that the article is still accessible on the news paper's website which was also positioned in the Google search engine. They sought a compensation together with an order to remove the article and publish again an apology by the newspaper. The national courts considered the issues involved in the second case were not *res judicata* due to the discovery a new source and a new claim. Nonetheless, it was found that removing the article from the website would not serve any practical purpose or offer adequate protection since the applicants have already received an apology. Furthermore, above-mentioned article had been placed in the archive of the website, reader could therefore aware that it was published in the past. Consequently, removing the article was considered that it would amount to censorship and to rewriting history.

The ECtHR focused on the balancing between the right to protection of private life under Article 8 and freedom of expression under Article 10 of the ECHR referring its jurisprudence.[228] It was highlighted that these provisions deserve equal respect.[229] The Court has previously held that the protection of private life has to be balanced, among other things, against the freedom of expression guaranteed by Article 10 of the Convention, in particular, in cases concerning newspaper publications.[230] The significant role of the freedom of expression was emphasized stating that the measures guaranteed to the press and careful scrutiny under Article 10 are particularly important.[231] To limit the access of public to the information, particularly strong reasons must be provided.[232] On the other hand, the freedom of press must have certain limits if the reputation and rights of others are at stake.[233]

The Court drew attention the difference between the Internet as an information and communication tool and the printed media considering the capacity to store and transmit information. It was found that "*the risk of harm posed by content and communications on the Internet to the exercise and enjoyment of human rights and freedoms, particularly the right to respect for private life is certainly higher than that posed by the press."* According to the case-law of the Court, Article 10 covers also the legitimate interest of the public in access to the public internet archives and particularly as they are readily accessible to the public and are free, they constitute an important source for education and historical research.[234]

The refusal of the courts to order the withdrawal of an article damaging the reputation of a lawyer and available in a newspaper's Internet archives was found not to be in breach

[228] Von Hannover v. Germany, App. No. 59320/00, 2004-VI Eur. Ct. H.R., and Karakó v. Hungary, App. No. 39311/05, Eur. Ct. H.R., (2009).

[229] Hachette Filipacchi Associés (ICI PARIS) v. France, App. No. 12268/03, Eur. Ct. H.R., (2009), and Timciuc v. Romania, App. No. 28999/03, Eur. Ct. H.R., (2010) and Mosley v. the United Kingdom, App. No. 48009/08, Eur. Ct. H.R., (2011).

[230] Karakó Case, supra note 207; Armonienė v. Lithuania, App. No. 36919/02, Eur. Ct. H.R., (2008); Biriuk v. Lithuania, App. No. 23373/03, Eur. Ct. H.R., (2008), and Axel Springer AG v. Germany, App. No. 39954/08, Eur. Ct. H.R., (2012).

[231] Bladet Tromsø and Stensaas v. Norway, Application No. 21980/93, 1999 III Eur. Ct. H.R.

[232] Timpul Info-Magazin and Anghel v. Moldova, App. No. 42864/05, Eur. Ct. H.R., (2007).

[233] Tammer v. Estonia, App. No. 41205/98, 2001 I Eur. Ct. H.R., and Dalban v. Romania, App. No. 28114/95, 1999 VI Eur. Ct. H.R.

[234] Times Newspapers Ltd v. the United Kingdom, App. Nos. 3002/03 and 23676/03, Eur. Ct. H.R., (2009).

of Article 8 by the ECtHR. The Court accepted that publishing the article violated the applicants' rights, however the instant case in connection respect of the above-mentioned second set of civil proceedings required a different examination. In this regard, the presence of the offending article on the newspaper's website and the State's positive obligations under Article 8 of the Convention arising in this context were analyzed by the ECtHR.

In the first proceedings the applicant did not neither show nor even argue before the courts that they wished to be taken in respect of the internet publication with a view to securing the effective protection of their reputation. Unlike *K.U. v. Finland* case[235] such possibility was available to the applicants, but they chose not to do so. After an assessment of all circumstances, the Court accepted that ordering the removal from the public domain of all traces of publications which had in the past been found was not the role of the judicial authorities to engage in rewriting history. In conclusion, *"…a limitation on freedom of expression for the sake of the applicant's reputation in the circumstances of the present case would have been disproportionate under Article 10 of the Convention."*

As demonstrated in Chapter 5, compared to the *Google Spain* case given by CJEU[236], this decision could not go beyond mentioning the name of legitimate interest. Besides, no analysis that would suggest the protection of personal data or the right to be forgotten is included within the scope of privacy. Regarding the conclusions of this case, it can be predicted that the ECtHR is much more conservative in terms of technological developments and data protection law compared to the CJEU.

6.4 *Surikov v. Ukraine*[237]

Surikov decision is one of the ECtHR's decisions that includes the concept of legitimate interest in the processing of employees' data. It is closely related to the *Section 2.2.3 Relationship with special categories of personal data* in this study since the case analyses processing of data concerning health. In sum, the Court found a disproportionate interference with the applicant's right to respect for his private life due to the fact that

[235] K.U. v. Finland, App. No. 2872/02, Eur. Ct. H.R., (2008).
[236] Google Spain Case, supra note 122.
[237] Surikov v. Ukraine, App. No. 42788/06, Eur. Ct. H.R., (2017).

long-term retention of data regarding individual's mental health, its dissemination and further processing were not connected with initial reasons of collection.[238]

Surikov with a diploma in technical engineering asked for a promotion to an engineering position in his company and his demands were refused for the second time on the grounds of his mental health conditions. The information about him being unfit for military service in accordance with Article 5b of the then applicable 1973 Diseases and Handicaps Schedule issued by the Ministry of Defence of the Union of Soviet Socialist Republics in 1981 was accessed through his personnel file by the company. Afterwards, the human resources department obtained further explanation about his mental state with a certificate. The company defended itself stating that the employers should have discretion to decide whether the employees have the necessary personal skills to fit in related position in the company. The national court rejected the applicant's claim justifying the company's arguments finding no legal reason to oblige the employer to make the applicant's promotion. Surikov's application before national courts was seeking to oblige the company to promote him, to pay him non-pecuniary damages for the purportedly unlawful processing of his health data, libel, and discrimination on the basis of health. Then he amended his claim alleging that processing of his health data is in breach of Ukraine law.

ECtHR first referred relevant Council of Europe materials such as the Convention 108, the Charter, OECD Guidelines and the Directive stating data protection rules concerning particular case. After the confirmation of applicability, the Court gave an affirmative answer to the existence of an interference by a public authority with the applicant's exercise of his right to private life. As to the legitimate aim part, ECtHR stated this interference may have various legitimate aims such as protection of national security, public safety, health, and the rights of others, in particular of the applicant's co-workers as listing exceptions in second paragraph of Article 8 under ECHR. Then, two additional conditions must be fulfilled, in order to justify the interference, it must be shown that the interference is in accordance with law, and it is necessary in a democratic society. One of the critical points in the case that although there were some legal bases in Ukraine law accept that collection, storage, and other use of the applicant's mental health, it was not

[238] Guide, supra note 222.

convinced whether these laws have enough quality and consistent with international obligations. Therefore, without explicitly answering this question the Court continued to analyze the case.

The main focus of the Court was the necessity criterion in a democratic society in *Surikov* decision. In this regard, firstly, it analyzed the power of collection and retention of the applicant's personal data. According to the national law, since every employer kept a schedule which includes a reference to the grounds for dispensation from military service and this schedule can be accessed in public source, the Court considered the company competent to retain the data. However, considering legislative framework gives a quasi-automatic entitlement for any employer whether public or private, to obtain and retain sensitive health-related data concerning any employee dispensed from military service on medical grounds, it was not considered proportionate and complying with the principle of limited periods of data storage.[239] ECtHR further noted that this kind of automatic delegation to the employer can be justified under Article 8 only if the data processing activity was accompanied by certain guarantees which ensure data kept strictly confidential, would not be used for any other purpose except that for which it was collected, and would be kept up-to-date applicable law. These references made by the Court remind *Section 4.6. Additional Safeguards* which are considered crucial to comply with data protection principles under EU law. As mentioned above, although right to privacy is a negative right, when it comes to the protection of personal data, the Court places the right to protection of personal data, which is a positive right, into its traditional methodology, in which it examines a negative right. Thus, the ECtHR, like the CJEU, but with a different method, imposes an obligation on data controllers to take additional measures, in the frame of the condition of being necessary in a democratic society. In conclusion, the Court decided this broad entitlement of the employers was disproportionate and not necessary in a democratic society.

In respect of the disclosure of the applicant's data to third parties and using it for deciding on his promotion ECtHR made critical inferences regarding the legitimate interest. The Court recognized that employers may have a legitimate interest information concerning their employees' mental and physical health, in cases of assigning them

[239] S and Marper Case, supra note 212.

certain job functions specified skills, responsibilities or competences. Yet, it emphasized that the existence of a legitimate interest does not mean the data processing activity is legitimized, a fair balance between the employer's interests and the privacy-related concerns of the candidate for the relevant position must be struck. Exercising the balance, the Court found the related health data not up-to-date and accurate and incomplete for the purposes of deciding the applicant's promotion. In fact, while explaining about the data protection principles in *Section 2.2.1*, it was stated that all data processing activities should be in accordance with the data protection principles, regardless of which legal ground they are based on. Here, too, although the Court does not expressly state it, using the principles of accuracy and purpose limitation, it has decided that the data processing activity is against the general principles even though there is a legitimate aim, and at the end of the day, Article 8 is violated since the interference is not necessary in a democratic society.

Apart from the background check for promotion of employees, regular monitoring of employees is also one of the issues that are considered within the scope of legitimate interests. Employee monitoring for safety or management purposes was interpreted under a separate heading by WP29.[240] Legitimate interest ground was found appropriate legal ground for the systems of where billable hours worked by employees are followed and frequently used today for the purposes of both billing and bonus payment. Provided that the system is explained to employees giving the opportunity of disagreement with the conclusion, the processing was found necessary for the legitimate interest of the data controller. In addition, to achieve the purpose there does not appear to be a less intrusive way. On contrary, checking employees' internet use to control they do not make excessive personal use of the company's IT was considered disproportionate intrusion into the private life of employees. In this case, the data processed include temporary files and cookies embedded in the employees' computers which show visited websites and downloads performed during working hours. Noteworthy here is limiting the time spent by the employees visiting websites not directly relevant to their work, the methods used was found intrusive. As a best practice advised by WP29, the employers should discuss and agree with employees' representatives and communicate them in a transparent way.

[240] OPINION, supra note 21, at 62.

6.5 General Assessment

One of the most striking common points in the decisions summarized above is that the case law is mostly about sensitive personal data within the scope of legitimate interests. Thus, it becomes possible to see the change and development of the Court's perspective on the subject in the decisions examined in chronological order. First, in the *Yvonne Chave née Jullien* case[241], it was observed that the processing of this data met the legitimate interest of the public hospital service's effective running, and in this encounter, it was decided in favor of the data controller without focusing on the special nature of the mental health data. Second, in *S. and Marper* case[242], this time, there was prevention of crime against special categories of personal data namely DNA samples. However, the Court here made a much more careful evaluation and analyzed the nature of the DNA samples data and what kind of risks it entails. As a result of its analysis, the Court determined that the interference was disproportionate. Finally, in *Surikov* case[243], instead of public legitimate interest, private legitimate interest was in question. Even though it was accepted that the interference may have legitimate aims such as national security, public safety, health, and the rights of others, in particular of the applicant's co-workers, the measures taken by employer was insufficient in context of fair balance.

Another point that draws attention in the case law of ECtHR within the framework of legitimate interest is that, unlike the CJEU, the only criterion that it focuses on and finds worth examining is necessity, although the three cumulative legitimate interest criteria are mentioned. Deciding whether the interference is necessary in a democratic society, it generally focuses directly on the test of proportionality without examining whether the legitimate interest is real and present. In the balancing test, it can be clearly seen that it performs a much more superficial and inactive test compared to CJEU.

In *Węgrzynowski and Smolczewski* case[244], at the intersection of freedom of information and right to privacy, it is understood that ECtHR takes a rather conservative stance alongside the CJEU. Balancing the legitimate interest of the public in accessing information and the right to privacy of the data subject, the Court has never focused on

[241] Yvonne Chave née Jullien Case, supra note 221.
[242] S and Marper Case, supra note 212.
[243] Surikov Case, supra note 237.
[244] Węgrzynowski and Smolczewski, supra note 226.

the way the search engine works and has not examined any issue that touches the right to be forgotten. In this aspect, *Google Spain* Case has a much more innovative perspective.[245]

As for the review method of the Court, as mentioned above, ECtHR, which has the point of view that the right to protect personal data imposes positive obligations on States, determines whether these positive obligations are fulfilled by applying the fair balance test. The fair balance test aims to determine certain type of State action by comparing the general interest of the community with the interests of the individual. There are three stages in this test, first the reasonableness justification is examined, then the positive obligations of the State to protect the relevant right are determined and finally it is decided whether the state acts in accordance with these obligations.[246] Legitimate interest examination in personal data protection law and fair balance here have similar features. In both, different interests are weighed, and an evaluation is made according to the characteristics of the particular case. However, the factors affecting this balance are different. For example, the narrow or wide margin of appreciation of the government, the characteristics of the balanced interests, and the interference intrusiveness affect the fair balance test known as proportionality review.[247] Similarly, the nature of the data processed, the method of processing, the audience affected by the processing and the reasonable expectation of data subject are considered in the legitimate interest review. At the end of the day, additional safeguards are also effective in the examination of legitimate interests, and the ECtHR looks at these measures of the data controller in positive obligations cases. Although there are similar points, it cannot be said that the ECtHR's examination method is exactly the same as the legitimate interest examination method. It has already been mentioned that some biases may occur because the data protection review is privacy-based. Therefore, it is thought that it will be beneficial for the ECtHR to determine the fair balance factors and standards specific to the subject, as in expulsion cases[248], for legitimate interest cases within the scope of data protection, leaving the basis of privacy, and a more transparent process can be carried out.

[245] Google Spain Case, supra note 122.

[246] JANNEKE GERARDS, GENERAL PRINCIPLES OF THE EUROPEAN CONVENTION ON HUMAN RIGHTS 113-114, (2019).

[247] Id., at 242-250.

[248] Boultif v. Switzerland, App. No. 54273/00, Eur. Ct. H.R., (2001). Üner v. the Netherlands, App. No. 46410/99, Eur. Ct. H.R., (2006), Maslov v. Austria, App. No. 1638/03, Eur. Ct. H.R., (2008).

As a last point, data protection cases are one of the cases for the ECtHR to take express account of EU law, since they include fields for overlap between ECHR and EU law. Thus, a lack of cooperation between the two systems causes inconsistent case law or even conflicting obligations for the States.[249] To avoid such inconsistencies and informal discussions between the ECtHR and the CJEU, a solution can be found in harmonious interpretation or interpretation of ECHR provisions in the light of EU law.

[249] GERARDS, supra note 246, at 102.

Chapter 7: FUTURE OF LEGITIMATE INTEREST

7.1 *Challenges in information society*

7.1.1 General View

Important technological developments, which are closely related to each other, are divided in three waves by Webster: Agricultural revolution, industrial revolution and information revolution.[250] It was argued that to complete the latter one, information revolution, it needs to be pass four stages of computerization at the level of (1) big science, (2) management, (3) society and (4) the individual.[251] In Küzeci's opinion, the place of personal data in the change and transformation that causes a society to change its name and to be described as an information society is undeniable. resulting in the information society can be divided into three periods.[252] First, of course, with the development of computers and central data banks, the definitions of data warehouses and data banks emerged. With the information power in the hands of large companies and governments reaching serious levels, the information flow between the public and private sector has also accelerated, thus paved the way for the digital dossiers of individuals.[253]

The second major transformation has been with the internet, as can be expected. In this environment, where every movement produces data, two different methods of data processing emerged when serving commercial goals came into play.[254] The more commonly known method is to register on websites by entering the username and password. The second and more controversial method is the method of monitoring IP addresses or placing cookies while browsing the internet. Thus, commercial sites are provided with the opportunity to determine the consumption trends of their target audiences, to provide services in accordance with these trends and even to direct these trends. In addition to consumption trends, searches made in search engines, which are a

[250] FRANK WEBSTER, THEORIES OF THE INFORMATION SOCIETY 9, (1995)
[251] YONEJI MASUDA, THE INFORMATION SOCIETY AS POST-INDUSTRIAL SOCIETY 36, (1983).
[252] KÜZECİ, supra note 10, at 31.
[253] DANIEL J. SOLOVE, THE DIGITAL PERSON 3, (2004).
[254] KÜZECİ, supra note 10, at 36-41.

huge library, are also recorded for later use for advertising purposes. Detailed obligations regarding the search engines that are on the radar of WP29 are envisaged.[255]

With all these developments, the rapid development of the state's methods of intervening in internet communication has brought with it the third period: The era of new technologies that provide surveillance. We live in a surveillance society. "It is pointless to talk about surveillance society in the future tense."[256] Stating that we are now faced with a new type of surveillance with massive electronic surveillance activities like ECHELON[257], Marx said the distinguishing features of this surveillance are: It transcends distance, darkness and physical barriers; it transcends time; it has low visibility; it is often involuntary; prevention is a major concern; it is capital; it involves decentralized self-policing, it triggers a shift from targeting a specific suspect to categorical suspicion of everyone; it is more intensive and extensive.[258] This has revealed the necessity of the law of protection of personal data as a defense mechanism of the fears and anxieties of the individual who feels that he/she has become transparent against surveillance.[259]

When it comes to the private sector rather than the public authorities, a much more dangerous picture emerges. Since there is no sanction in the private sector, the personal data of individuals are mostly processed with voluntary participation.[260] The reason behind this may be to receive various services and promotions in line with the individual's own economic interests, as well as to transfer personal data to social networking sites as a requirement of participation in the social environment of the new century. However, it should be kept in mind that knowledge is a power and an individual who loses control over their personal information will become powerless. It is possible that the individual whose tastes, consumption habits, likes, preferences, socio-economic status and political thoughts are transferred to the digital environment cannot foresee the results of this processing. It becomes possible to access many details about a person's life with the

[255] Opinion 1/2008 on data protection issues related to search engines, 00737/EN WP 148 (Apr. 4, 2008).

[256] Information Commissioners Office, A Report on the Surveillance Society, (Sep. 2006), https://ico.org.uk/media/about-the-ico/documents/1042390/surveillance-society-full-report-2006.pdf.

[257] BRUCE SCHNEIER, SECRETS & LIES DIGITAL SECURITY IN A NETWORKED WORLD 35-56, (2004).

[258] GARY T. MARX, UNDERCOVER, POLIS SURVEILLANCE IN AMERICA 217-129, (1988).

[259] KÜZECİ, supra note 10, at 46.

[260] Id., at 55.

matching of the value obtained from different sources and automatic monitoring activities, also called dataveillance.[261]

Today, search engines provide access to data anytime and anywhere, on the other hand, individuals spread their thoughts to every corner of the world through social media. Online communication platforms enabling individuals to join or create networks of like-minded users, namely Social Networking Services, individuals are encouraged to provide personal data and create their profile.[262] By this way, companies benefit from effective and efficient marketing techniques that boost the economy. Besides, state authorities fight against crime and terrorism with the help of data processing.[263] Similarly, identifying patterns and predicting behaviors through big data are considered as a significant value for society, public sector performance and social participation.[264] However, the methods of collecting and processing personal data result in heated debates since massive data sets can be easily cross-checked and further analyzed to look for patterns or for the adoption of decisions on algorithms.[265] The fact that these data sets include unprecedented information about human behavior and private life constitute a big challenge in information technologies world. Mass surveillance activities by state agencies can have a negative effect on the right to privacy, democracy, creativity, and innovation given that they can discourage citizens from expressing their views and cause wariness and caution.[266] Not only on public but also on private side, corporations which can reach massive data sets may reveal health and financial data of individuals for their economic benefits.

It is obvious that the challenges that arise with the effect of technology require a different benefit-risks assessment from the cases described in the previous sections, and therefore will play a critical role in the legitimate interest analysis that is the subject of this thesis. One of the reasons behind this difference is the volume and variety of data.[267] As European Parliament identified, since "a lack of methodology to make an evidence-

[261] Roger Clarke, http://www.rogerclarke.com/DV/.
[262] Opinion 5/2009 on online social networking, 01189/09/EN WP 163 (Jun. 12, 2009).
[263] HANDBOOK, supra note 170, at 347.
[264] Council of Europe, Consultative Committee of Convention 108, Guidelines on the protection of individuals with regard to the processing of personal data in a world of big data, (Jan. 23, 2017).
[265] European Parliament, Resolution on fundamental rights implications of big data: privacy, data protection, non-discrimination, security and law enforcement, (March 14, 2017).
[266] Digital Rights Ireland Case, supra note 121.
[267] Resolution, supra note 265.

based assessment of the total impact of big data" exists, "measuring exactly the extent to which privacy and personal data may be affected is not possible."[268] Another aspect of the difference of the modern technological challenges is the results of the processing activity.[269] One of the most difficult issues is to determine who the controllers and processors are and the limits of their liabilities. As to the impact on data protection principles, it can be said that the fair and transparent process has never been more critical before. Individual control becomes more and more important. In this regard, to inform data subject granting the rights to access, rectify, erase, restrict and object to the processing data is crucial.

In this study, the personal data processed with unpredictable methods in the age of information technologies and the effects of this situation on economic and social life have been tried to be mentioned from time to time. In this part of the study, these effects will be examined in more depth and additional attention will be drawn to the points that touch the legitimate interest in relation to the subject of the thesis.

7.1.2 Prevention of Fraud and Blacklist Threat

It is explicitly stated that "the processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the data controller concerned" under 47. Recital of the GDPR. Even though the legitimate interest clause under Article 6/1/(f) of the Regulation includes the word of "necessary", in cases of preventing fraud it is required that the data processing activity is "strictly necessary". Therefore, it is required a stricter review to exercise balancing test in context of fraud.

Since the Directive did not mention expressly that the purposes of prevention of fraud constitute a legitimate interest, the practical examples of WP29 helped as a guide. Financial institutions which verify and record the identity information of the persons who want to open an account may rely on the legitimate interest ground provided that they follow reasonable and proportionate procedures in the WP29's opinion.[270] However, it must be kept in mind that, if the actions of financial institutions are specifically defined under national applicable law, then the processing activity should be relied on the legal

[268] Id.
[269] HANDBOOK, supra note 170, at 355.
[270] OPINION, supra note 21, at 61.

obligation clause. For instance, under Turkish law, since the Law No. 5549[271] and its sub-regulations[272] clearly specify the conditions under which the identification and verification of the customer should be carried out within the framework of the principle of knowing your customer, the said data processing activities of financial institutions, which are among the obligations, consist of fulfilling their legal obligations. In respect of financial institutions, exchanging data regarding suspected abuse of anti-money laundering rules with other companies within the same group was considered as another example of cases reliable on the legitimate interest clause.[273] Obtaining advice of the competent data protection authority and applying strict limitation on access, security and prohibition of any further use are clearly favorable factors to decide the applicability of legitimate interest. In the Regulation, under 48. Recital, it is stated that "controllers that are part of a group of undertakings or institutions affiliated to a central body may have a legitimate interest in transmitting personal data within the group of undertakings for internal administrative purposes, including the processing of clients' or employees' personal data." Although in these cases, there are no internal administrative purposes, fighting money laundering was deemed to be a legitimate interest according to the WP29.

In order to prevent fraud and money laundering within the same group, it brings up the issue of information sharing between different organizations, which is one step beyond information sharing. As in the law numbered 5411 under Turkish law, the exchange of all kinds of information and documents between banks and financial institutions, directly or through companies to be established by a risk center or at least five banks or financial institutions under certain conditions may be permitted and can be evaluated under legal obligation clause of the Regulation. However, if such an obligation does not exist, information sharing between organizations can only be considered as a legitimate interest for certain purposes and if certain conditions are met. The fact that information sharing among different institutions, also called blacklist, can be used for discrimination has also brought many sensitive debates in the fields concerning fundamental rights. Processing certain information belonging to a particular group within

[271] Law No. 5549 on Prevention of Laundering Proceeds of Crime, Article 3 and Article 8.

[272] Regulation on Measures Regarding Prevention Of Laundering Proceeds Of Crime and Financing Of Terrorism (Jan. 9, 2008), https://ms.hmb.gov.tr/uploads/sites/2/2019/04/ROM_amended_10_june_2014-1-1.pdf. MASAK General Communique No 19. (Apr. 30, 2021), https://masak.hmb.gov.tr/masak-genel-tebligi-sira-no-19/.

[273] OPINION, supra note 21, at 62.

the criteria of a list can be useful in measuring the credibility of individuals, preventing fraud cases, and providing more effective protection for a specific sector or public interest such as blacklists on administrative offences or employment records. However, on the other hand, it can create adverse or prejudicial effects for the specific group in the list, resulting in the other group individuals being prevented from accessing any goods or services or damaging their reputation. Leaving citizens vulnerable in that they have themselves no knowledge that their personal data have been entered on a blacklist because these were obtained from another source breaches not only the data protection principles but it may also constitute a violation of the prohibition of discrimination under Article 14 of the ECHR.

Entering individuals onto databases on which they are identified in connection with a specific situation or specific facts represents an intrusion is defined as "blacklist".[274] WP29 explains that two important aspects of blacklists are their prejudicial effects and clear discrepancies among Member States. On the one hand, it is very difficult to determine the concept and the nature of blacklists, on the other hand they may discriminate against a group of people by barring them access to a specific service or harming their reputation, therefore they must comply with the data protection principles.

7.1.2.1 Financial Data

Blacklists which include financial data are one of the most known and common blacklists used by states. Financial data may contain solvency and credit information of individuals which indicate the individual's financial capacity assuming a future credit commitment. As a second possibility, blacklists including financial data may provide information on the breach of monetary obligations of individuals. Depending on whether an individual has failed to meet previous obligations, a negative rating for subsequent credit is possible. An interesting point is that, even if the files contain only positive background of individuals and they seem like they have no stigmatizing purpose, since they have positive discrimination effect stating that anyone on the list is good, anyone who is not is bad, or at least suspect, their frequent use may also have a negative effect on individuals. According to the WP29, these kinds of blacklists should have its basis in legislation for instance making it possible for the competent financial authorities to assess the general

[274] Working Document on Blacklists, 11118/02/EN/final WP 65, (Oct. 3, 2002).

risk assumed by financial concerns or in the data subject's free, unequivocal, specific, and informed consent.

While the creditor's files are related to a specific debtor's contractual relationship, in joint files, the data controller is a body which provides solvency and credit rating information to which the creditor supplies the data, also known as "bad debt files". Generally, several bodies in single or multiple sectors enter into an agreement with a third undertaking with an aim of communicating the records of customers who default on loans to that undertaking. Joint files which include persons who have failed at any time properly to meet their previous financial commitments must be relied on either specific contract clauses authorizing the creditor to disclose the data on the outstanding debt to a joint file or on the data controller's legitimate interest.

It is not surprising that WP29 lists the data protection principles to comply with for legitimate interest clause regarding the balancing of interests. However, up-to-date principle other than accuracy and transparency is the most emphasized principle on the subject. An obligation is clearly imposed on data controller “to reflect the fact that the debt has been paid off even if the entry on non-payment is maintained beyond the date of full repayment.” For up-to-date principle, it is advised to define general parameters for standardizing the times for which the data contained on files may be kept or blocked. Concerning the quality of data, a definite due debt must have remained unpaid, and the debtor must have received a reminder requiring him to make the payment. The obligation to inform data subjects since the very moment of the inclusion of their personal data in the common file is also significant. Besides, recognizing the right of access to the data, right to correct and right to erase when notifying the inclusion is indispensable. Technical and organizational security measures and conditions must be provided accessing to data. Also, it must be avoided errors in identifying the individuals included (such as data subjects with common names), in including debts under discussion with the data subject and in references to the number of debts. In order to correct immediately any error of this kind as soon as it is detected, it must be set up cautious verification instruments.

Another important aspect of this kind of file concerns individual automated decision. Both the Directive under Article 15 and the Regulation under Article 22 recognize that individuals have right not to be subject to a decision on automated

processing. It is listed contractual relationships, legislations which provide suitable measures to safeguard the data subject's rights and freedoms and legitimate interests and explicit consent of data subjects as exceptional cases parallel with the Directive. Regarding automated decisions, the GDPR also included profiling in the clause and decision-making for fraud and tax-evasion monitoring and prevention purposes conducted in accordance with the regulations under 71. Recital. It must be born in mind that the data subjects must be provided information about the existence of automated decision making to ensure fair and transparent process.

7.1.2.2 Criminal Offences

In general, criminal convictions and offences can only be processed under the control of an official authority under both Article 8(5) of the Directive and Article 10 of the Regulation. The files including criminal offences or convictions are legitimized by the obligation of authorities to maintain security and public order, therefore it is relied on the public task clause which concern processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

However, it was detected that in private sector, such as large supermarkets or vehicle rental firms, personal data on “undesirable customers” is being collected and processed. WP29 stated that which persons and institutions may have access to these data are included in the penal laws of the member countries and may differ from each other, while referring to the principles of protection of personal data and stated that the whole process should be designed in accordance with these principles.[275] At this point, as an example, criminal conviction records, which were accessed by the employee upon the request of the employer, were shown and it was stated that the use of the employer in the selection process would not constitute a contradiction, but further use of these records manually or automatically could create a contradiction.[276]

After the title of financial data and criminal offences, it would be appropriate to mention a blacklist that serves both purposes. Early Warning System (EWS) is an internal

[275] Id.
[276] Id.

information tool that helps the European Commission and its executive agencies to identify third parties that pose financial and/or other risks.[277] All public authorities which implement EU funds can access Central Exclusion Database based on the Regulation No 1302/2008.[278] The database includes all companies, organizations or natural persons excluded from EU funding on the grounds of insolvency or criminal convictions. It is aimed to ensure the sound financial management of European Union funds and to prevent fraud. In the Opinion of the European Commission regarding the processing operation on personal data concerning the "Registration of a Data Subject in the Central Exclusion Database", it is explained what criteria should be considered when reviewing this type of blacklist.[279] In this regard, prior check was made by evaluating not only the lawfulness of the processing and the quality of data; but also retention period, time limit to erase data, rights of data subject, storage and security measures.

7.1.2.3 Fraud detection

Apart from the 47th recital, which clearly accepts fraud prevention as a legitimate interest in GDPR, identity theft and fraud as well as discrimination and financial loss were counted among the serious consequences that data processing and violations can cause in 75th and 85th recitals. From this point of view, it can be said that fraud is a concept that should be evaluated on two facets, both as a threat that will arise as a result of not protecting personal data effectively and as one of the purposes of protecting personal data.

To clarify the concepts, identity theft or identity fraud which is the most rapidly growing type white-collar criminal activity is defined as 'stealing' another person's personal identifying information and then using that information to fraudulently establish credit, run up debt, or take over existing financial accounts by U.S. General Accounting Office.[280] While an ordinary cart fraud, a thief steals and uses a person's credit cart, identity theft steals personal information and may use in many fraudulent ways.[281] Public

[277] https://edps.europa.eu/data-protection/data-protection/reference-library/blacklisting-and-early-warning-systems_en

[278] European Commission and EURATOM, Regulation No 1302/2008 on the central exclusion database, (Dec. 17, 2008).

[279] European Commission, Opinion on a notification for Prior Checking received from the Data Protection Officer regarding the processing operation on personal data concerning the "Registration of a Data Subject in the Central Exclusion Database", (Case 2009-0681), (May 26, 2010).

[280] GAO Identity Theft Report

[281] SOLOVE, supra note 253, at 110.

records are very useful to help verify individual identity and investigate different types of fraud.

Data processing for fraud prevention is usually carried out by law enforcement authorities. Law enforcement agencies have long sought personal information about individuals from various companies and financial institutions to investigate fraud. Under Article 58/1/e of the GDPR each supervisory authority shall have the investigative powers of obtaining of personal data from the controller and the processor and accessing to all personal data and to all information necessary for the performance of its tasks. For instance, Regulatory DataCorp (RDC)) which was created by many of the world's largest financial companies has offered a massive database about people opening new bank accounts. Through its database, namely Global Regulatory Information Database (GRID), information to provide financial companies background checks of potential customers for fraud, money laundering, terrorism, and other criminal activity has been gathered.[282] However, it should be born in mind that the data protection principles still need to be complied even though it was relied on this article. RDC was unable to correct the errors in case that some information in the database may be incorrect result in incompatibilities with the principles such as accuracy and transparency.[283]

One step beyond data processing to prevent fraud is automated investigations and profiling created by the related authorities. In 1977, the Federal Government of the United States began matching its computer employee records with those of people receiving federal benefits. Investigating millions of people with the use of computers to match records of different government entities to detect tax, welfare, and food stamp fraud as well as to identify drug couriers normally constitutes a violation of the Privacy Act. In contrast, it was justified under the "routine use" exception. Since the meaning of routine use was stretched, it raised significant concerns.[284] Therefore, Congress finally passed a law regulating this practice.[285]

[282] https://docs.dnb.com/onboard/en-US/Business/RDC#GRIDDatabase
[283] SOLOVE, supra note 253, at 21.
[284] Marx, supra note 258, at 209-120.
[285] Computer Matching and Privacy Protection Act (CMPPA) of 1988, Pub. L. No. 100-500, 102 Stat. 2507.

It should be noted that fraud cases have a special place not only for public authorities but also for some private companies. Some sectors experience fraud more intensely compared to other sectors and prevention of fraud cases is of great importance for the continuity of the sector such as insurance sector. In these cases, joint files help the companies to combat fraud techniques and reduce their operating costs. Information about clients suspected of fraud or action in breach of the related provisions of the sector can be used for further decisions of companies.

Yet, the cases where insurance companies centralize data on the number of damages related to a client in a certain period of time no matter what responsibility the client has, may have non-compliance aspects with data protection legislation unless legal provisions specifying adequate guarantees under national law exist.[286] Exercising of the right of access, notification of the data subject, conservation of the data for a specified period with the purpose for which they are collected and the obligation to erase data are in line with what is described in bad debt files.

The involvement of fraud detection with personal data has also been subject to the case law of CJEU and ECtHR. In *Schwarz v. Stadt Bochum* case, taking and storing of fingerprints to issues passports was analyzed by CJEU in the frame of prevention of fraud answering the question of whether Article 1 (2) of Regulation 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States is valid.[287] The limitation of the right to personal data protection was found provided by law since it was designed to prevent the falsification of passports and their fraudulent use. Therefore, it was stated that the provision pursued an aim of the general interest recognized by the EU namely preventing illegal entry to the EU. Therefore, the limitation was considered appropriate for the aim pursued as it reduces the related risk significantly. Considering necessity, since only alternative method to the fingerprint was seen iris scan and this method is not yet advanced and significantly more expensive, also no inference can be made that the iris scan method is less interfering, this criterium was found fulfilled. The Court further noted that the Regulation constituted a legal basis only for verifying the authenticity and identity, not for the centralized storage of the data.

[286] European Commission, supra note 275.
[287] Case C-291/12, Michael Schwarz v. Stadt Bochum, 2013 E.C.R.

In two cases that the ECtHR dealt with the question of whether the strictions to professional secrecy constitute an infringement of Article 8 of the ECHR indirectly with the issue of prevention of fraud. In *Pruteanu v. Romania*, the ECtHR held that there had been a violation of Article 8 of the ECHR with his client regarding the interception of a lawyer's conversations following allegations of fraud.[288] In *Brito Ferrinho Bexiga Villa-Nova v. Portugal* case, again concerning a lawyer following an investigation for tax fraud, the Court considered that the interference had a legal basis and pursued legitimate aim.[289] However, examining the necessity and proportionality of the interference, since the applicant had no knowledge about the procedure due to the lack of procedural guarantees and effective judicial control over the measure suspending the duty of confidentiality, the ECtHR concluded that there had been a violation.

In conclusion, although it is clear that fraud detection is possible in cases where data processing is strictly necessary under GDPR, whether the data controller is public authority or private company, the nature of the processed data, the method of transferring data, appropriate measures taken and whether there is a data processing in accordance with the principles within the scope of the protection of personal data will decide the result of the balance test.

7.1.2.4 Other categories

Although it is not included in the frequently used categories described above, it can also be met with blacklists in different categories that require special protection. These lists containing special categories of personal data. It is known that most Member States permit processing of special categories of personal data only if there is an explicit consent of the data subject or set out strict requirements.

In context of health data, the companies offering life insurance may have lists containing such personal data of their customers if legal regulations have the appropriate measures. If there aren't any legal regulations, data subject must be given his/her explicit consent which he/she is entitled to revoke. Joint files centralized by a federation of insurance companies which included data on persons who had been refused life insurance

[288] Pruteanu v. Romania, App. No. 30181/05, Eur. Ct. H.R., (2015).
[289] Brito Ferrinho Bexiga Villa-Nova v. Portugal, App. No. 69436/10, Eur. Ct. H.R., (2015).

on the grounds of their health problems was considered in breach of data protection principles by some national supervisory authorities as they considered that the nature of the contractual relationship between life insurance company and customer could not provide grounds for holding this information.[290]

In the same vein, the registers, or public files of individuals whose conduct is considered dangerous considering social and political behaviors, it must be grounded on legal provisions for compiling these also specify the safeguards and the restrictions on access to the data. When the social and political behaviors at stake, the conflicts between the right to privacy of individuals on these lists and the right to freedom of expression of those circulating them may appear. As it was explained the intersections between two rights under section 6.3 in a detailed way, it is not possible to make a general standardization between these rights. However, even though freedom of expression is a widely interpreted right, it cannot cause the principles of protection of personal data to be disregarded such as principles of proportionality, up-to-date and exercise of the right of access, the right to rectify and to erase data. If these are refused, WP29 imposes the obligation of offering an opinion on the data protection supervisory authorities.[291]

Under the title of other blacklisting categories, it can be considered a joint blacklist of aggressive drug addicts created by a group of hospitals in order to prohibit them accessing to all medical premises of the participating hospitals.[292] On the one hand, maintaining safe and secure premises may constitute a legitimate interest, on the other hand such interests can be overridden by the right of access to health treatment of the data subjects. The fact that processed data includes special categories of personal data, it is unlikely to apply the legitimate interest clause in this case. In the case where a legal provision exists providing specific safeguards such as checks and controls, transparency, prevention of automated decisions ensuring that it would not result in discrimination or violation of fundamental rights of individuals, then legitimate interest clause may come into the stage. It is obvious that, if this specific law requires the data processing, it must

[290] Id.
[291] Id.
[292] OPINION, supra note 21, at 62.

be relied on legal obligation clause, but if it only permits the data processing, legitimate interest clause can be relied on depending on the facts of the particular case.[293]

As an important example that enables the evaluation of the blacklisting by the national data protection authority is the car rental decision given by the Turkish DPA and published as a principal decision in Official Gazette.[294] Car rental companies use a software provided by a software company which record all the data obtained from their customers accessible to all other car rental companies users. By evaluating the operation and control of the software used, the finding that both car rental companies and software companies are joint data controllers on customers' personal data is noteworthy.[295] However, the fundamental point of the decision considering legitimate interest companies claim that they use this program to reach the customers, inform them about campaigns and send informative messages at the delivery point. In addition, the program serves as a warning system which contain comments about customers who pose a problem renting a car. It was stated that the system gathers car rental companies under one roof providing information flow and ensuring customer satisfaction. The part up to this point indicates the existence of legitimate interests of companies. In the decision, it has been concluded that if the company using the software would make use of this database alone, the balance test may result in favor of the data controller, according to the conditions of the concrete case. In contrast as the personal data of the customers are accessed and processed by other car rental companies using the software without their consent, it violates their fundamental rights.[296]

As a result of the transition from physical records to digital records, personal data protection law can be used as an effective tool in order to prevent the unlimited processing of personal data in a world where control is not that easy. As can be seen, the processing of financial data, criminal conviction data and other sensitive data could be possible by legal obligations and contract performance grounds before, but now these different types and numbers of data associated in various manners cannot be framed by these grounds. Since the only remaining clause is legitimate interest, it is possible for this door not to

[293] Id.

[294] Principal decision of Turkish DPA on the blacklist practices in the car rental industry, (Jan. 20, 2022), https://www.resmigazete.gov.tr/eskiler/2022/01/20220120-10.pdf.

[295] Id.

[296] Id.

remain open all the time and thus to ensure the balance in both economic and social fields. Of course, for this, it should be detected carefully where the legitimate interest begins and ends and on what issues it may surface, how the purposes such as prevention of fraud or maintaining security can be abused by the data controllers and how the data subjects can be protected in the most effective way. After answering these, it will be easier to cope with the challenges of the future.

7.2 *Pursuing legitimate interest with direct marketing purposes*

7.2.1 General information

Under 47. Recital of the GDPR, it is explicitly stated that the processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest. In order to leave no room for doubt, the regulator clearly places an activity within this scope in a matter such as legitimate interest, which is unclear how it will be shaped in practice. Besides, under 70. Recital of the Regulation, the right to object of data subject is emphasized when data is processed with direct marketing purposes. The data subject should have the right to object on profiling to the extent that it is related to such direct marketing, whether with regard to initial or further processing, at any time and free of charge. Therefore, it is necessary to develop a sound understanding about the extent of direct marketing, when the profiling starts and ends to inform data subject in an appropriate way.

The notion of direct marketing may cover many different types of marketing practices in today's world. Therefore, to clarify its scope, WP29 has divided direct marketing into conventional direct marketing and other forms of marketing in terms of legitimate interest.[297] Obtaining the contact details of the customers by a computer store and process them for marketing by regular mail of its own similar products and send promotional e-mails when a new product line comes into stock is considered conventional direct marketing. It is assumed that there are not any complex profiles created by the company such as analyzing of customer's click-stream data. In this case, the customers can reasonably except to receive these e-mails for similar products as a customer of the shop. Thus, it can be based on the legitimate interest ground. WP29 points out that

[297] OPINION, supra note 21, at 60.

informing clearly about right to object of customers, free of charge and in an easy manner and the transparency of the processing constitute the elements to reach this conclusion. As another example, using the data retaining from electoral register by a candidate to send an introduction letter promoting his/her campaign to each potential voter in his/her district is deemed to be appropriate example of legitimate interest. Assuming the application of the electoral register is established by law, the interest of controller is found clear and legitimate. Provided that the data processed is limited and focused, such use falls into the scope of reasonable expectations of data subjects, here citizens.

The criterium of reasonable expectation has also the aspect of time. The Belgian DPA decided recently that direct marketing messages may be sent to former customers for legitimate interest in certain circumstances.[298] 47. Recital of the GDPR and its recommendation relating to the processing of personal data personal for direct marketing purposes[299] were based on defining these circumstances. Accordingly, when determining whether there is a legitimate interest or not, it should be evaluated whether it can reasonably expect that the data of the persons concerned may be processed for such a purpose at the time and context of the data collection. In the particular case, since the relationship between the data controller and the data subject ended about two years ago and the data subject did not object to the processing during this period, it was decided that it could still be considered within the scope of reasonable expectation and the complaint was rejected.

On the other hand, data matching from different sources and creating a profile does not fall into the scope of the conventional direct marketing. To illustrate, an online pharmacy carrying out marketing which process data about medicines and other products that customer purchased or obtained by prescription combines this information with demographic information of customers such as age and gender.[300] In addition, the click stream data of customers is processed while browsing on the website. Consequently, a health and wellbeing profile of customers is created which include predictions about

[298] Decision 117/2022 of Belgian DPA, (July 22, 2022) https://gdprhub.eu/index.php?title=APD/GBA_(Belgium)_-_117/2022&mtc=today

[299] Belgian Data Protection Authority, Recommendation 01/2020 relating to the processing of personal data personal for direct marketing purposes*, (*Jan. 17, 2020), https://www.autoriteprotectiondonnees.be/publications/recommandation-n-01-2020.pdf.

[300] OPINION, supra note 21, at 59.

being pregnant, suffering from a particular illness, interest in dietary supplements etc. After analyzing this data, the pharmacy uses it to offer non-prescription medicines, health supplements and other products to its customers. In this example, legitimate interest ground cannot be applicable in many ways. First, the marketing activity involves sensitive data, and many people would not reasonably expect that this information is processed purchasing in an online pharmacy shop. Second, the extent and manner of profiling that uses predictive algorithms results in a high level of intrusiveness.

Similarly, collecting information for targeting purposes sometimes may cause excessive data processing. As an example, a non-profit-seeking body collects data on its social networking sites about liked or shared messages the organization posted, regularly viewed or re-tweeted.[301] Then it sends messages and newsletters to its members according to their profile to carry out fundraising activities. Elderly dog owners who liked articles on animal shelters receive different fundraising appeals from families with small children. Besides, people from different ethnic groups also receive different messages. As it is a philosophical organization, it processes special categories of data such as philosophical beliefs. In the Regulation parallel with the Directive special categories of personal data may be processed in the course of the legitimate activities with appropriate safeguards by an association. However, WP29 found this condition not sufficient for a lawful processing. As explained in Section 2.2.3 the specific requirements under special categories of data does not exclude the general principles and the conditions for lawful processing. In this case the way that the data is processed, the amount of data collected and the lack of transparency about the reuse of data exceeds the reasonable expectations of its members, and it can only be relied on the explicit consent.

7.2.2 FEDMA's Code[302]

Federation of European Direct Marketing (FEDMA) whose members are the Direct Marketing Associations of 12 countries of the European Union (all except Belgium, Luxembourg and Denmark) and Switzerland, Norway, Hungary, Poland, the Czech and Slovak Republics prepared FEDMA's Code which was designed primarily as an instrument of best practice.

[301] OPINION, supra note 21, at 60.

[302] Federation of European Direct Marketing, European Code of Practice for the Use of Personal Data in Direct Marketing, (June 12, 2017).

The significance of the document comes from the broad definition of direct marketing. It was defined as "the communication by whatever means (including but not limited to mail, fax, telephone, on-line services etc.) of any advertising or marketing material, which is carried out by the Direct Marketer itself or on its behalf and which is directed to particular individuals."[303] The criteria of obtaining personal data, responsibilities of data controller and even specific provisions for children are explained in the document. For fair processing, data subjects should be essentially informed about data controller's identity and the purpose of the processing activity. In addition, data controllers must ensure that data subjects are informed of their right to access and correct erroneous data related to them; their right not to be approached for direct marketing purposes; their right to object to the processing of his/her personal data for direct marketing purposes.

In FEDMA's Code, it was stated that if the data is processed for a different purpose than the first notified purpose, an evaluation should be made over the new purpose. Accordingly, if the new purpose is compatible with the first notified purpose, there is no obstacle to data processing anyway. However, if it is not compatible then further assessment is required. The questions of "whether the new purpose(s) is substantially different from the purpose(s) for which data were collected, whether data subjects could reasonably have foreseen or whether it is probable that they would have objected to if they had known" should be answered and a final analysis should be made accordingly.

Concerning the security measures employed by the data controllers, controllers are encouraged to use specific measures, such as Privacy Enhancing Technologies (PETs),[304] and seeding lists. The written convention between the list-broker and the list user should ensure that lists are used with respect to appropriate security principles. Besides, the security of the buildings in which the personal data are stored and/or processed, list of authorized persons with a mention of their liability to access the data, appropriate authentication mechanisms such as passwords control, and security in the

[303] Id.

[304] Communication From the Commission to the European Parliament and The Council on Promoting Data Protection by Privacy Enhancing Technologies (PETs), COM(2007) 228.

transfer of data between the data controller and the data processor are fundamental criteria to ensure carrying out lawful data processing.[305]

7.3 *Profiling and Behavioral Targeting*

One step beyond the pursuing legitimate interest for direct marketing purposes, and a more dangerous future dimension is profiling and behavioral targeting. Today's marketing industry is passionate about behavioral targeting focusing on user experience. Mark Wilmot explains the beginning of this era with these words probably with no expectation about this potentially dangerous practice in the future:

"Something amazing happens when marketing efforts are actually relevant to people. We see this step as initiating that crucial dialogue. And shoppers, for their part, are replying; essentially giving permission to marketers to learn their habits and respond accordingly."[306]

Even though something amazing happened in marketing industry as Wilmot claimed, individuals and organizations face complex, sometimes intangibles, and often ambiguous trade-offs. Individuals have many doubts on whether the security of their data is provided and the misuse of information they pass to other entities is avoided. In contrast, they are also eager to share their personal data with peers and third parties' information that makes mutually satisfactory interactions possible. Organizations want to know more about the parties they interact with day by day, tracking them across transactions. Yet, they do not want to use invasive policies that complicate customer experience.[307]

One of the most effective tools that enables profiling and behavioral advertising is big data. Big data is defined by International Telecommunications Union as "a paradigm for enabling the collection, storage, management, analysis and visualization, potentially

[305] FEDMA's code, supra note 293, at 11.

[306] Mark Wilmot, *Put Out the Welcome Mat,* Marketing Daily, (July 28, 2009), https://www.mediapost.com/publications/article/110489/put-out-the-welcome-mat.html.

[307] Alessandro Acquisti, The Economics of Personal Data and the Economics of Privacy' (Background Paper for the Conference: The Economics of Personal Data and Privacy: 30 Years after the OECD Privacy Guidelines) (2010).

under real-time constraints, of extensive datasets with heterogeneous characteristics."[308] Despite the different definitions of big data depending on the specific disciplines, most of them focus on "the growing technological ability to collect process and extract new and predictive knowledge from great volume, velocity, and variety of data."[309] Although the detailed analysis of the effect of big data on the protection of personal data goes beyond the scope of this thesis, in the part of legitimate interest, it is desired to draw attention to the effect of these concepts brought by technology to the subject.

A new quantitative dimension of data which can be evaluated and used in real time can be used to deliver tailored services to consumers thanks to big data. Behavioral trackers gather data from people browsing the web and use that data to tailor the information that those people receive usually with economic interests.[310] The data processed is not limited with the websites visited, but it also includes when, how, what links are followed, every click made and the timing between them.[311] All these gathered information can be analyzed, and profiles can be created based on their behaviors.

Profiling is one of the processes that may rely on automated decision-making according to predetermined patterns or factors.[312] Obtaining consent of data subjects and individuals in big data processing presents a challenge for data protection law. Here the consent covers both the consent to being subject to tailored advertisements and profiling and the consent to the use of masses of personal data to refine and develop information-based, analytical tools.[313] As it can be seen, regarding the profiling and targeted advertising, the fundamental points are the awareness and the control of individuals on their data. It may not necessarily be a problem if individuals are aware that they are subject to tailored adverts. However, profiling, and targeted advertising will cause problems in context of rights of individuals when it is used for the manipulation them. For instance, emotion-detection techniques which use facial expressions and voices to infer emotional states are increasingly available to merchants. Besides the effects on

[308] International Telecommunications Union, Recommendation Y.3600 (11/2015), Big Data – Cloud computing based requirements and capabilities, https://www.argentina.gob.ar/sites/default/files/2021/04/recomendacion_uit-t_y.3600_-_big_data.pdf

[309] Council of Europe, Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data, (Jan. 23, 2017).

[310] PAUL BERNAL, INTERNET PRIVACY RIGHTS 144, (2014).

[311] Id.

[312] HANDBOOK, supra note 170, at 351.

[313] Id., at 360.

commercial domain, rumors or fake new may also be disseminated through manipulative platforms. Pleasing or exciting individuals, confirming their biases, triggering negative feelings and provide symbolic rewards and punishments are certain methods to canalize people with the help of behavioral targeting.[314] As to the political arena, for example, groups of undecided voters can be addressed via political messages tailored to their "personality" and attitudes.[315]

Combination of personal information across web services is one of the most used tools to guarantee best possible quality of service by companies today. Internet companies have started to offer various services to users including search engines, video sharing or social networking. Online advertising sector is mainly based on the arrangements which advertisers pay website publishers if somebody clicks on ad. As a type of electronic marketing, behavioral targeting involves three parties namely an Internet user, a website publisher, and an advertising network. Advertising networks use tracking cookies to recognize people when they visit websites and show related ads for instance ads for hotels for somebody who is profiled as a travel enthusiast.[316] Developing a privacy policy with a clause stating it will combine all personal information without any data retention period cannot be sufficient for users to have an individual control over specific combinations of their data. WP29 found an imbalance between company's legitimate interests and data subjects' rights in these cases.[317] Thus, in its view, the only way out for these companies is considered an informed consent provided that other principles are met.

Advertising network providers are bound by Article 5(3) of the ePrivacy Directive.[318] The ePrivacy Directive requires informed consent processing data by placing cookies or similar devices on users' terminal equipment or obtaining information through such devices. To be able to obtain an informed consent, WP29 imposes on the advertising network providers the obligation of creating prior opt-in mechanisms which needs an affirmative action by the data subjects indicating their willingness to receive cookies or

[314] Study of the European Parliament, Regulating targeted and behavioural advertising in digital services, How to ensure users' informed consent, (Sep. 2021).

[315] Id.

[316] Frederik J. Zuiderveen Borgesius, *Personal data processing for behavioural targeting: which legal basis?* International Data Privacy Law, 5(3), 163-176, (2015).

[317] OPINION, supra note 21, at 68.

[318] The European Parliament and The Council, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), (July 12, 2002) (amended in 2019).

similar devices and the subsequent monitoring of their surfing behavior for the purposes of serving tailored advertising.[319] Advertising "network providers should i) limit in time the scope of the consent; ii) offer the possibility to revoke it easily and iii) create visible tools to be displayed where the monitoring takes place" to maintain the awareness of the data subjects.[320] Due to the nature of the behavioral advertising the principle of transparency and providing clear and comprehensive information play a key role processing data.

However, Borgesius argued that in some cases it can be relied on the necessity for performing a contract as a legal basis, as the 'contract' would imply that the user discloses personal data, in exchange for using the social network site.[321] When the user opens an account in a social network site, it may be defended that behavioral targeting is necessary for the performance of the contract. In the same direction, European social network providers have suggested that behavioral targeting is necessary for a contract:

"Whether analyzing user data for ad targeting or suggesting individual services is lawful is a controversial topic. We would highly appreciate if the future legal framework for processing of user data would clarify that these ways of analyzing and using user data do not necessarily require consent but rather are part of the processing that is necessary for the performance of a contract to which the data subject is party."[322]

Concerning the possibility of relying on the legitimate interest ground in behavioral targeting cases, unlike WP29, it was implied that there are alternatives to consent by the ICO.[323] It is presumed that the ICO hinted at necessity for the controller's legitimate interests as a possible legal basis.[324] It has been confirmed that online marketing relates to the freedom to conduct a business by Advocate General by the CJEU.[325] As known, having a legitimate interest is not sufficient to be relied on this ground. It seems

[319] Opinion 2/2010 on online behavioral advertising, 00909/10/EN WP 171, (June 22, 2010).
[320] Id.
[321] Borgesius, supra note 316.
[322] European Social Networks, 'Response to the Commission's Public Consultation on the Comprehensive Approach on Personal Data Protection in the European Union' (14 January 2011) https://panoptykon.org/sites/default/files/Response%20EU%20commission.pdf.
[323] Information Commissioner's Office, 'Personal Information Online. Code of Practice' (2010) ,https://ico.org.uk/media/for-organisations/documents/ 1591/personal_information_online_cop.pdf
[324]
[325] Google Spain Case, supra note 122.

questionable whether tracking people's browsing behavior is the least restrictive manner for the ad network to enable advertisers to promote their products. For instance, contextual advertising is another method possible to display related ads without tracking people's behavior such as ads for law books on websites about law. On the other hand, an ad network that specializes in behavioral targeting could try to argue that tracking people is necessary for its business.[326] Therefore, the fulfillment of the necessity criterium will be dependent on the circumstances of the particular case. Concerning the principle of the proportionality, since behavioral targeting requires mostly large-scale data protection this criterium appears not easy to be passed. Yet, some practical architectures such as Adnostic which is a browser plug-in which enables targeting without compromising user's privacy building a profile based on the user's browser. [327] Lastly, balancing the interests, it is accepted that people have a reasonable expectation of privacy on Internet use confirming by the ECtHR.[328] In addition, there are various factors that should be taken into account such as the seriousness of the infringement of the data subject's fundamental rights, the sensitivity of the data, the scale of data collection, and the risks involved.[329]

In a recent case from State Commissioner for Data Protection in Germany it was examined that a bank obtaining a meaningful data set through its mobile applications by comparing information such as purchasing volume, frequency of use of bank statement outputs, transfer amount, both with the data in the same category in its branches and with the data of a credit institution.[330] It was explained that the purpose of this processing activity is to identify customers who have an increasing inclination towards digital media and to use electronic communication channels more to deal with contractual or advertising purposes. Even though general information was given to the customers on the subject, their explicit consent was not obtained. The State Commissioner decided that the data controller failed the balance test that must be applied within the scope of legitimate interest under Article 6/1/(f) of the Regulation. Due to the data analysis enriched with the information received from the branches and the credit institution, the processing activity

[326] Borgesius, supra note 316.

[327] S Barocas and others, 'Adnostic: Privacy Preserving Targeted Advertising' (2010), https://crypto.stanford.edu/adnostic/adnostic-ndss.pdf.

[328] Copland v United Kingdom, App No. 62617/00, Eur. Ct. H.R., (2007).

[329] OPINION, supra note 21, at 33-43.

[330] https://lfd.niedersachsen.de/startseite/infothek/presseinformationen/900-000-euro-bussgeld-gegen-kreditinstitut-wegen-profilbildung-zu-werbezwecken-213925.html

exceeded the reasonable expectations of the customers. At this point, the quote from Data Protection State Commissioner Barbara Thiel is noteworthy:

"The data controllers for such evaluations often do not obtain the consent of the customers. Instead, they refer to a balancing of interests according to the Article 6/1/f. However, this legal basis does not allow profiles to be created for advertising purposes by evaluating large databases… Those data subjects usually do not expect data controllers to use databases on a large scale to identify their inclination towards certain product categories or communication channels."[331]

As can be understood, the debate on behavioral targeting and necessity for the controller's legitimate interests as a legal basis has not been settled. In conclusion, the challenges awaiting the information society in the future is mentioned at every possible opportunity focusing on the fact that they change and deepen the personal data protection law in many aspects and may even leave it inadequate at some points. However, it cannot be denied that the issue has a more sensitive point when viewed from the perspective of legitimate interests. One of the most emphasized issues from the starting point to the conclusion of the thesis is that legitimate interest is a clause used by both the public and private sectors when the other legal grounds are not applicable. As such, technological developments have changed the methods of processing personal data, making it much more complex and chaotic, and the decrease in predictability in legal texts and contracts in this context, all eyes have turned to the legitimate interest clause. Since it is known that seeing any field as a way out usually results in abuse, it has been tried to convey which issues and purposes should be considered in this section. Financial data, data on criminal offences and sensitive personal data require a delicate balance, especially when it comes to fraud or security purposes. When the economic interests are mentioned, it is useful to carefully evaluate profiling and behavioral advertising methods.

[331] Id.

Chapter 8:
CONCLUSION

This thesis is a study that evaluates the past, present, and future of the concept of legitimate interest in order to shed light on its unclear aspects. At the end of the review, it was aimed to find an answer whether the legitimate interest clause provides an effective protection today and whether it will be an effective tool in the future. Recognizing both the opportunities that legitimate interest clause offer to the data controllers and the risk of their abuse of this clause provided an opportunity to make an overall assessment and detect problematic issues on the subject. The subjectivity of the balancing test which involve subjective questions such as the impact on the data subject or the seriousness of the infringement open up grey areas. It has been observed that even though the literature and case-law tend to turn a subjective notion into the objective assessment to provide clear answers, the room for abuse still remain. Embracing subjectivity and grey areas may be an option just as GDPR did. Yet, it has been witnessed that this option is not sufficient to create an efficient tool in data protection.

Structurally, first of all, the appearance of the notion of legitimate interest has been researched and for this, the milestones of personal data law and international sources have been scanned for this purpose. Here, in fact, it is seen that legitimate interest has taken its place in the present sense in the Directive, based on the principles of fairness and lawfulness that existed before. Therefore, it should not be forgotten that there are basic principles at the core of this legal ground. At this point, the use of fairness under Article 5/1/a of the Regulation may be an effective provision for data controllers throughout decision making process to explain how and why they process data in a structured and explicit way.

As the process of transition from Directive to the Regulation from the past to the present is of great importance in terms of legitimate interests, this transformation has been tried to be evaluated in detail. In this context, it is understood that the reason

behind the conscious choice of legal instrument is the goal of harmonization considering the specific characteristics of the EU legal order. It is undeniable that GDPR serves this purpose more than the Directive, as there are criticisms that there is a serious lack of legal certainty in terms of legitimate interest in the texts examining the implementation of the Directive. It should be aware of this important step for the legitimate interest clause to provide effective protection, but there are also reservations about whether it is sufficient.

In the second place, it is known that contextualization is essential in order to understand the positioning of legitimate interest in personal data law, thus the relationship between this clause and other provisions of the GDPR has been tried to be revealed. In this regard, it was concluded that all the other data protection principles, especially proportionality, purpose limitation and transparency, should be considered together so that legitimate interest can create optimum balance with a holistic approach. Referring to the initial question, it is essential for effective protection that these principles are reflected in legitimate interest practices. However, it is not always easy to detect these principles scattered throughout the text including related recitals. Hence, it would be useful to review all the principles for each case.

Thirdly, the problem of lack of legal certainty, which is one of the centering points of the thesis, has been examined. Unfortunately, it is understood that the choice of legal instrument is not sufficient in solving this problem and it is related to the inherent flexibility of the legitimate interest clause. No one had much idea about the effects and consequences of this clause, which was created by those who prepared the Regulation to form a space for the data controller. It should be realized that this dilemma is not specific to the legitimate interest clause. There is a danger that all the provisions of the national or international authorities, which draw a general framework, will go away from legal certainty in practice. This is a choice of law-making method, choosing a casuistic method and limiting all legitimate interest cases by enumeration is another method, while drawing a general framework and leaving the rest to jurisprudence and practice can be another choice. The question of which choice provides more effective protection leads to a much older debate, which is of no use to the subject. Instead, it is questionable whether a case law and doctrine has been developed that provides effective protection on the subject in a way that prevents abuse of this lawmaking

technique. At this point, the related cases in CJEU and ECtHR case law were examined. Looking at the decisions examined, it is undoubted that both courts helped to develop doctrines on legitimate interest and to provide certainty in practice. However, it can be said that the examination of only issues such as establishment of legal claims, video surveillance or economic interest with CJEU decisions is rather barren when compared to legitimate interest practices. ECtHR, on the other hand, has lagged even further behind the CJEU, has not yet escaped from the privacy point of view and has remained rather timid in examining data protection law. Consequently, the only remaining tool on how to provide effective protection may be the recommendations and guidelines of the relevant EU authorities.

Documents published by some EU authorities, starting with WP29 and followed by EDPS, are the most useful tools in this context. At least, these documents were able to create some benchmarks especially for data controllers by following the latest developments. Yet, the challenges of the information society mentioned in the last chapter seem to affect the areas of use of legitimate interests the most among the legal grounds. Aside from the general threat of personal data in profiling and behavioral advertising with big data, attention has been drawn to the fact that legitimate interest is more vulnerable among other legal grounds. The most useful element that can prevent this vulnerability will be additional safeguards, as expressed in many parts of the study. On the one hand the additional safeguards may tip the balance in favor of the data controller showing the efforts made to provide an effective protection. On the other hand, they will become more difficult to fulfill as the expectations from the data controller will increase under the title of additional safeguard considering the negative effects and threats on the data subject,. The close relation between the impact on the data subject in the particular case and the importance of the additional safeguards demonstrates that technical and operational measures will become much more important in the future. Using of anonymization techniques, privacy-enhancing technologies and opt-out processing will help to comply with the principles of accountability and transparency. In fact, in a sense, there is an irony that the challenges created by technology are eliminated with the opportunities provided by technology. Even today, it is not known where the personal data processed with unpredictable numbers and different methods will reach, and it is very difficult to raise awareness despite all procedures and policies. As long as the information given is manipulative

and the measures taken are forged, it will be easy to be convinced of the legitimacy of the interests of the companies. On top of that, failing to draw the framework of safeguards at times when big data, artificial intelligence and robots will come into play may easily cause balance tests to be abused in favor of data controllers. Ultimately, balancing the information asymmetry between the data subject and the data controller as one of the ways to prevent uncontrolled power in the new world where information is the real power.

In this study, in addition to giving a negative answer to the issue of whether the legitimate interest provides effective protection today, it has been tried to give a warning that this protection will be even more inadequate in the future. To eliminate the negative effects of future challenges, legitimate interest clause under GDPR needs to be reviewed in the light of new technological developments and the decisions of the CJEU and the ECtHR, which will become deeper day by day. In this context, of course, it is not possible to list all criteria depending on the circumstances of the cases in the Regulation. Instead, it should be designed linking the balance test of the legitimate interest clause to objective questions on the additional safeguards without leaving a right of choice to the data controller according to the particular case. Besides, there is an inconsistent and confusing language such as strictly necessary, under its recitals in statements that prevent fraud and direct marketing purposes may create legitimate interest. In this context, even if these recitals can be considered to provide some clues, no guidance was given as to when these purposes could pass the balancing test. For topics such as fraud, blacklisting, profiling, and behavioral targeting, which will become even more debated in the future, a regulation that is both flexible and compatible with technology and in which a certain framework is drawn should be targeted. In line with this goal, the relevant international sources, data protection authorities' decisions and case law should be examined, and appropriate criteria should be listed for these topics under separate headings in the Regulation.

BIBLIOGRAPHY

A. Books

Alexy, Robert. The Oxford Handbook of Comparative Constitutional Law, (Michel Rosenfeld & Andras Sajo eds. 2012).

Berlin, Isaiah. Liberty (Henry Hardy ed. 2002).

Bernal, Paul. Internet Privacy Rights (2014).

Bygrave, Lee A. Data Privacy Law An International Perspective (2014).

Develioğlu, Hüseyin M. 6698 Sayılı Kişisel Verilerin Korunması Kanunu ile Karşılaştırmalı olarak Avrupa Birliği Genel Veri Koruma Tüzüğü Uyarınca Kişisel Verilerin Korunması Hukuku (2017).

European Union Agency for Fundamental Rights and Council of Europe, Handbook On European Data Protection Law (2018).

Gerards, Janneke. General Principles of the European Convention on Human Rights (2019).

Heisenberg, Dorothee. Negotiating Privacy, The European Union, the United States, and Personal Data Protection (2005).

Hizarci, Emine. 6698 Sayılı Kişisel Verilerin Korunması Kanununun AB Veri Koruma Hukuku Işığında Değerlendirilmesi (2020).

Işık, Sezen K. Avrupa Veri Koruma Hukukuna Anayasal Bir Bakış (2020).

Kuner, Christopher, Bygrave, Lee A., Docksey, Christopher, eds., and Drechsler, Laura, asst. ed. The EU General Data Protection Regulation (GDPR). A Commentary (2020).

Küzeci, Elif. Kişisel Verilerin Korunması (2021).

Lynskey, Orla. The Foundations of EU Data Protection Law (2015).

Masuda, Yoneji. The Information Society as Post-Industrial Society (1983).

Marx, Gary T. Undercover, Polis Surveillance in America (1988).

Purtova, Nadezhda. Property Rights In Personal Data A European Perpsective (2012).

Schneier, Bruce. Secrets & Lies Digital Security in a Networked World (2004).

Solove, Daniel J. The Digital Person (2004).

Voigt, Rüdiger. Legalität Ohne Legitimität: Carl Schmitts Kategorie Der Legitimität (2015).

Webster, Frank. Theories of the Information Society (1995).

Westin, Alan. Privacy and Freedom (1967).

B. Articles

Balboni, Polo, Cooper Daniel, Imperiali, Rosario & Macenaite, Milda. *Legitimate interest of the data controller New data protection paradigm: legitimacy grounded on appropriate protection,* International Data Privacy Law, Vol. 4, pp. 244-161 (2013).

Bloustein, Edward. *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*, New York University Law Review, Vol. 39, (1964).

De Hert, Paul & Gutwirth, Serge. *Data protection in the case law of Strasbourg and Luxemburg : constitutionalisation in action*, Reinventing Data Protection? Vrije Universiteit Brussel From the Selected Works of Serge Gutwirth, Vol.6, pp. 3-44 (2009).

De Hert, Paul & Papakonstantinou Vagelis, *The new General Data Protection Regulation: Still a sound system for the protection of individuals?,* Computer Law & Security Review, Vol. 32, pp. 179-194 (2016).

El Emam, Khaled & A´lvarez, Cecilia. *A critical appraisal of the Article 29 Working Party Opinion 05/2014 on data anonymization techniques*, International Data Privacy Law, Vol. 5, pp. 73-87 (2015).

Fuster & Gellert, *The fundamental right of data protection in the European Union: in search of an uncharted right*, International Review of Law, Computers & Technology, Vol. 26, pp. 73-82 (March. 2012).

Hofnagle, Chris J., Van der Sloot, Bart & Borgesius, Frederik Z. *The European Union general data protection regulation: what it is and what it means*, Information & Communications Technology Law, Vol. 28, pp. 65-98 (2019).

Hustinx, Peter. *EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation* (Sep 15, 2014).

Kamara, Irene & De Hert, Paul. *Understanding the balancing act behind the legitimate interest of the controller ground: A pragmatic approach*, Vol.4, No.12, (Aug, 2018).

Kang, Jerry. *Information Privacy in Cyberspace Transactions*, Stanford Law Review, Vol. 50, pp.1193-1294 (1998).

Lessig, Lawrence. *Privacy as Property,* Social Research, Vol. 69, pp. 247-269 (2002).

Poullet, Yves. *The Directive 95/46/EC: Ten years after,* Computer Law & Security Report Vol. 22, pp. 206-127 (2006).

Prins, Corien. *Property and Privacy: Perspectives and the Commodification of our Identity,* Kluwer Law International, Vol. 16, pp. 223-257 (2006).

Prins, Corien. *When personal data, behavior and virtual identities become a commodity: Would a property rights approach matter?*, Script – ed, Vol. 3(4), pp. 270-303 (June, 2006).

Prosser, William. *Privacy*, California Law Review, Vol. 48, pp. 383-423 (1960).

Salom, Javier A. *A third party to whom data are disclosed': A third group among those processing data*, International Data Privacy Law, Vol. 4, pp.177-188 (2014).

Samuelson, Pamela. *Privacy as Intellectual Property?,* Stanford Law Review, Vol. 52, No. 5, Symposium: Cyberspace and Privacy: A New Legal Paradigm? pp. 1125-1173 (May, 2000).

Schwartz, Paul M. Property, *Privacy and Personal Data*, Harward Law Review, Vol. 117, No. 7 pp. 2056-2128 (May, 2004).

Şakar, Mehmet C. *Carl Schmitt'te Yasallık Ve Meşruluk Üzerine Bir İnceleme*, (2017).

Warren, Samuel D. & Brandeis, Louis D. *The Right to Privacy,* Harward Law Review, Vol. 50, pp. 194-221 (1890).

Wrigley, Sam. *Bots and AI-Related Technologies, Legitimate Interest, And Fair Processing under The General Data Protection Regulation,* (Dec 17, 2021).

Zittrain, Jonathan. *What the Publisher Can Teach the Patient: Intellectual Property and Privacy in an Era of Trusted Privication*, The Berkman Center for Internet & Society at Harward Law School (March 9, 2000).

Zuiderveen Borgesius, Frederik J. *Personal data processing for behavioural targeting: which legal basis?* International Data Privacy Law, Vol. 5, No. 3, pp. 163-176 (2015).

C. Opinions

Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC 844/14/EN WP 217 (Apr. 9, 2014).

Opinion of the European Data Protection Supervisor on the Final Report by the EU-US High Level Contact Group on information sharing and privacy and personal data protection (2009/C 128/01).

Opinion 12/2011 smart metering 00671/11/EN WP 183 (Apr. 4, 2011).

Opinion of the European Data Protection Supervisor on the data protection reform package (March 7, 2012).

Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector 536/14/EN WP 211 (Feb. 27, 2014).

Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT) 01935/06/EN WP 128 (Nov. 22, 2006).

Opinion 03/2013 on purpose limitation, 00569/13/EN WP 203 (Apr. 2, 2013).

Opinion 1/2010 on the concepts of "controller" and "processor" 00264/10/EN WP 169 (Feb. 16, 2010).

Opinion 3/2012 on developments in biometric technologies 00720/12/EN WP 193 (Apr. 27, 2012),

Second Opinion 4/2009 on the World Anti-Doping Agency (WADA) International Standard for the Protection of Privacy and Personal Information, on related provisions of the WADA Code and on other privacy issues in the context of the fight against doping in sport by WADA and (national) anti-doping organizations 0746/09/EN WP 162 (Apr. 6, 2009).

Opinion 05/2014 on Anonymisation Techniques 0829/14/EN WP216 (Apr. 10, 2014).

Opinion 1/2008 on data protection issues related to search engines, 00737/EN WP 148 (Apr. 4, 2008).

Opinion 5/2009 on online social networking, 01189/09/EN WP 163 (Jun. 12, 2009).

European Commission, Opinion on a notification for Prior Checking received from the Data Protection Officer regarding the processing operation on personal data concerning the "Registration of a Data Subject in the Central Exclusion Database", (Case 2009-0681), (May 26, 2010).

Opinion 2/2010 on online behavioral advertising, 00909/10/EN WP 171, (June 22, 2010).

D. Internet Sources

Barocas, Solon, Toubiana, Vincent, Narayanan, Arvind, Boneh, Dan & Nissenbaum, Helen. 'Adnostic: Privacy Preserving Targeted Advertising' (2010).

Council of Europe. New Technologies: A challenge to privacy protection? (Jan 20, 1988).

Complaint against Norwegian DPA, date of access 23.12.2022, https://gdprhub.eu/index.php?title=Datatilsynet_(Norway)_-_19/02450.

Future of Privacy Forum and Nymity innovating compliance. Processing Personal Data on the Basis of Legitimate Interests under the GDPR Practical Cases, (Sep. 4, 2022).

Robinson, Neil, Graux, Hans, Botterman Maarten & Lorenzo Valeri. Review of the European Data Protection Directive (May,2009).

Wilmot, Mark. Put Out the Welcome Mat, Marketing Daily, (July 28, 2009).

E. Legal Documents

1. Treaties and Conventions

Charter of Fundamental Rights of the European Union, 2000 O.J. C 364/01.

Consolidated Version of the Treaty on the Functioning of the European Union, 2012 O.J. C 326/47.

Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Jan. 28, 1981, E.T.S. 108.

Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community, , 2007 O.J. (C 306) 1.

2. Directives and Regulations

Directive (EU) 2016/680 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (27 April 2016).

Directive 2002/58/EC of the European Parliament and the European Council, concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (July 12, 2002).

European Commission and EURATOM, Regulation No 1302/2008 on the central exclusion database, (Dec. 17, 2008).

The European Parliament and The Council, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic

communications sector (Directive on privacy and electronic communications), (July 12, 2002) (amended in 2019).

Regulation on Measures Regarding Prevention of Laundering Proceeds of Crime and Financing of Terrorism (Jan. 9, 2008).

F. Other

Acquisti, Alessandro. The Economics of Personal Data and the Economics of Privacy' (Background Paper for the Conference: The Economics of Personal Data and Privacy: 30 Years after the OECD Privacy Guidelines) (2010).

Belgian Data Protection Authority, Recommendation 01/2020 relating to the processing of personal data personal for direct marketing purposes (Jan. 17, 2020).

Communication From the Commission to the European Parliament and The Council on Promoting Data Protection by Privacy Enhancing Technologies (PETs), COM(2007) 228.

Council of Europe. Consultative Committee of Convention 108, Guidelines on the protection of individuals with regard to the processing of personal data in a world of big data (Jan. 23, 2017).

Council of Europe. Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data, (Jan. 23, 2017).

Decision 117/2022 of Belgian DPA, (July 22, 2022).

European Commission. Comparative Study of Different Approaches to New Privacy Challenges, in Particular in the Light of Technological Developments (Jan.20, 2010).

European Commission. Letter to the Dutch Data Protection Authority, (March 6, 2020).

European Commission, Commission Staff Working Document […] Accompanying the document Communication from the Commission to the European Parliament and the Council: Data Protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation {COM(2020) 264 final}.

European Court of Human Rights. Guide to the Case-Law of the of the European Court of Human Rights Data protection (Aug. 31, 2022).

European Data Protection Board. Guidelines 4/2019 on Article 25 Data Protection by Design and by Default Guidelines, (Nov 13, 2019).

European Parliament. Resolution on fundamental rights implications of big data: privacy, data protection, non-discrimination, security and law enforcement (March 14, 2017).

European Social Networks. Response to the Commission's Public Consultation on the Comprehensive Approach on Personal Data Protection in the European Union (14 January 2011).

Federation of European Direct Marketing, European Code of Practice for the Use of Personal Data in Direct Marketing, (June 12, 2017).

Information Commissioner's Office. Guide to the General Data Protection Regulation, Lawful Basis for Processing, Vital Interests.

Information Commissioner's Office. Guide to the General Data Protection Regulation, Individual Rights, Right to data portability.

Information Commissioner's Office. Guide to the General Data Protection Regulation, Children.

Information Commissioners Office. Guide to the General Data Protection Regulation, Accountability and Governance.

Information Commissioners Office. Guide to the General Data Protection Regulation Principle (a): Lawfulness, fairness and transparency.

Information Commissioners Office. A Report on the Surveillance Society (Sep. 2006).

Information Commissioner's Office. 'Personal Information Online. Code of Practice' (2010).

International Telecommunications Union, Recommendation Y.3600 (11/2015), Big Data – Cloud computing based requirements and capabilities.

Organization for Economic Cooperation and Development (OECD). Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (Sept. 23, 1980).

Organization for Economic Cooperation and Development (OECD). Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (as amended on July 11, 2013).

Kamara, Irene. The Court of Justice of the EU: what to expect after the General Data Protection Regulation?, Workshop on: 'European Courts, New Technologies and Fundamental Rights' - Athens, Greece, (Jan. 2017).

Principal decision of Turkish DPA on the blacklist practices in the car rental industry (Jan. 20, 2022).

Study of the European Parliament. Regulating targeted and behavioural advertising in digital services, How to ensure users' informed consent (Sep. 2021).

Reding, Viviane. *The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the. Munich: Innovation Conference Digital, Life, Design Munich* (Jan 22, 2012)

MASAK General Communique No 19. (Apr. 30, 2021).

Working Document on Blacklists, 11118/02/EN/final WP 65, (Oct. 3, 2002).

The Commission of the European Communities. First report on the implementation of the Data Protection Directive (95/46/EC) (May 15, 2003).

The European Parliament and of The European Council. Proposal for a Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (Jan. 25, 2012).

The European Parliament and of the Council Committee on Civil Liberties, Justice and Home Affairs. Draft Report on the proposal for a regulation on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (Dec 17, 2012).

The European Data Protection Supervisor, Developing a 'toolkit' for assessing the necessity of measures that interfere with fundamental rights (Jun. 16, 2016).

The European Data Protection Supervisor. Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit (Apr. 11, 2017).

The United Nations Human Rights Committee. General Interpretation Number, (1988).

World Economic Forum in collaboration with Bain & Company, Inc., Personal Data: The Emergence of a New Asset Class 5 (Jan, 2011).

G. Case law

1. Court of Justice of the European Union

Case T-26/62, NV Algemene Transport- en Expeditie Onderneming van Gend & Loos v Netherlands Inland Revenue Administration, 1963 E.C.R. 00003.

Case T-41/74, Yvonne van Duyn v Home Office, 1974 E.C.R. 01337.

Leander v. Sweden, App. No. 9248/81, Eur. Ct. H.R. (ser A.), (1987).

Burghartz v. Switzerland, App. No. 16213/90, Eur. Ct. H.R. (ser. A), (1994)

Friedl v. Austria, App. No. 15225/89, Eur. Ct. H.R. (ser. A), (1995).

Joined cases Case C-465/00, C-138/01 and C-139/01, Rechnungshof v Österreichischer Rundfunk and Others and Christa Neukomm and Joseph Lauermann v Österreichischer Rundfunk, 2003 E.C.R. I-04989.

Case C-101/01, Lindqvist, 2003 E.C.R. I-12971.

Case C-73/07, Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy, 2008 E.C.R. I-09831.

Case C-553/07, College van burgemeester en wethouders van Rotterdam v M. E. E. Rijkeboer, 2009 E.C.R. I-03889.

Joined cases C-92/09 and C-93/09, Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen, 2010 E.C.R. I-11063.

Joined Cases C-468/10 and C-469/10, Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) (C-469/10) v. Administración del Estado, 2011 E.C.R. I-12181.

Case C-70/10, Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM), 2011 E.C.R. I-11959

Case C-342/12, Worten — Equipamentos para o Lar SA v Autoridade para as Condições de Trabalho, 2013 E.C.R.

Case C-291/12, Michael Schwarz v. Stadt Bochum, 2013 E.C.R.

Joined Cases C 293/12 and C 594/12, Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, 2014 E.C.R.

Case C 131/12, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, 2014 E.C.R.

Case C-212/13, František Ryneš v Úřad pro ochranu osobních údajů, 2014 E.C.R.

Case C-362/14, Maximillian Schrems v Data Protection Commissioner, 2015 E.C.R.

Case C-582/14, Patrick Breyer v Bundesrepublik Deutschland, 2016 E.C.R.

Case C-398/15, Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v Salvatore Manni, 2017 E.C.R.

Case C-13/16, Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v Rīgas pašvaldības SIA "Rīgas satiksme", 2017 E.C.R.

Case C-708/18, TK v Asociaţia de Proprietari bloc M5A-ScaraA, 2019 E.C.R.

Case C-40/17, Fashion ID GmbH & Co.KG v Verbraucherzentrale NRW eV, 2019 E.C.R.

2. European Court of Human Rights

Yvonne Chave née Jullien v. France, App. No. 14461/88, Eur. Ct. H.R., (1991).

Niemietz v. Germany, Eur. Ct. H.R. (1992).

Murray v. the United Kingdom, Eur. Ct. H.R. (1994).

Z v. Finland, App. No. 22009/93, 1997-I Eur. Ct. H.R.

Bladet Tromsø and Stensaas v. Norway, Application No. 21980/93, 1999 III Eur. Ct. H.R.

Dalban v. Romania, App. No. 28114/95, 1999 VI Eur. Ct. H.R.

Tammer v. Estonia, App. No. 41205/98, 2001 I Eur. Ct. H.R.

Coster v. the United Kingdom, App. No. 24876/94, Eur. Ct. H.R., (2001).

Boultif v. Switzerland, App. No. 54273/00, Eur. Ct. H.R., (2001).

Pretty v. The United Kingdom, App. No. 2346/02, 2002-III Eur. Ct. H.R.

Mikulić v. Croatia, App. No. 53176/99, 2002-I Eur. Ct. H.R.

Connors v. the United Kingdom, App. No. 66746/01, Eur. Ct. H.R., (2004).

Sciacca v. Italy, App. No. 50774/99, 2005-I Eur. Ct. H.R.

Üner v. the Netherlands, App. No. 46410/99, Eur. Ct. H.R., (2006).

Copland v United Kingdom App No. 62617/00, Eur. Ct. H.R., (2007).

Evans v. the United Kingdom, App. No. 6339/05, 2007 I Eur. Ct. H.R.

Timpul Info-Magazin and Anghel v. Moldova, App. No. 42864/05, Eur. Ct. H.R., (2007).

Armonienė v. Lithuania, App. No. 36919/02, Eur. Ct. H.R., (2008)

Biriuk v. Lithuania, App. No. 23373/03, Eur. Ct. H.R., (2008)

K.U. v. Finland, App. No. 2872/02, Eur. Ct. H.R., (2008).

Maslov v. Austria, App. No. 1638/03, Eur. Ct. H.R., (2008).

S. and Marper v. The United Kingdom, App. Nos. 30562/04 and 30566/04, 2008 Eur. Ct. H.R.

Von Hannover v. Germany, App. No. 59320/00, 2004 VI Eur. Ct. H.R., and Karakó v. Hungary, App. No. 39311/05, Eur. Ct. H.R., (2009).

Hachette Filipacchi Associés (ICI PARIS) v. France, App. No. 12268/03, Eur. Ct. H.R., (2009)

Times Newspapers Ltd v. the United Kingdom, App. Nos. 3002/03 and 23676/03, Eur. Ct. H.R., (2009).

Timciuc v. Romania, App. No. 28999/03, Eur. Ct. H.R., (2010)

Mosley v. the United Kingdom, App. No. 48009/08, Eur. Ct. H.R., (2011).

Axel Springer AG v. Germany, App. No. 39954/08, Eur. Ct. H.R., (2012).

Węgrzynowski and Smolczewski v. Poland, App. No. 33846/07, Eur. Ct. H.R., (2013).

Pruteanu v. Romania, App. No. 30181/05, Eur. Ct. H.R., (2015).

Brito Ferrinho Bexiga Villa-Nova v. Portugal, App. No. 69436/10, Eur. Ct. H.R., (2015).

Surikov v. Ukraine, App. No. 42788/06, Eur. Ct. H.R., (2017).