THE LAW OF COMMERCIAL PROFILING

A Thesis submitted for the Degree of Doctor of Laws

by

Elena A. Georgiou

Department of Law, Brunel University London

To my special friend Maria and to the memory of my grandmother Eleni

Acknowledgments

I would like to express my sincere gratitude to all the people who have supported and guided me throughout my study. My major debt is to my parents, Andreas and Niki. Without the support of both, it would have been difficult to produce this thesis. To Mr. Federico Ferretti, my supervisor, I am grateful for his constant support and expertise in the preparation of my thesis. I would also like to thank my friend Marilena Aristidou and Mr. Theodoros Chiou for giving their comments on the substance of the thesis. Finally, warm thanks are also due to my special friends Christina Sorokou, Constandinos Morphi and George Laskaris for supporting me in some difficult moments of this work.

Elena A. Georgiou

2018

Contents

Abstract

New technological developments and the large amount of databases nowadays enable the use of profiling practices which collect, combine, analyse and automatically categorise data into groups. This automatic categorisation and identification of individuals' data enables business and governmental entities to classify individuals into certain profiles. Although such resulting profiles can help business entities to identify current or potential targets for their own benefits and decision-makings, profiling is likely to generate certain prejudicial treatments for the individuals, which may threaten their privacy and data protection rights, as personal and sensitive information may be revealed. By monitoring all individuals' activities, profiling enables different types of information to be merged to link to individuals' offline lives and thus to their physical identities. As such, profiling challenges the protection of individuals' fundamental rights and values and creates conditions for surveillance, manipulation, threats to individuals' autonomy, discrimination, de-individuation, stigmatisation, stereotyping and inaccuracy in the decision process. In addition, the asymmetries of knowledge and the unbalanced distribution of powers between the controllers and the data subjects are likely to affect the individuality of a person and generate concerns over their autonomy and their right to self-determination. Privacy and data protection are recognised as legal instruments which protect the rights of the individuals to preserve their freedom to develop their own unique identities and individuality within society. This thesis is limited to profiling practices operating in the private sector for commercial purposes. Extensive use has been made of primary sources, such as legislation, and other secondary materials, such as journals and textbooks, for the preparation of this thesis. The findings of this thesis argue that profiling contradicts the idea of transparency and the self-determinatory (controllable) nature of data protection legislation, and thus of the GDPR. In practice, the law is ineffective to safeguard the protection of individuals' fundamental rights to privacy and data protection in the context of profiling: consent as a control mechanism has proven to be a pseudo-right under which individuals are giving their consent mechanically and unconsciously and thus it cannot be considered as the freely given, specific, informed and unambiguous indication of the individuals' wishes; the de-individuated character of profiling makes individuals

who have no interest either in exercising such control or to live a self-determined existence, and what is more, individuals are neither aware, nor able to be aware, that they are in this situation; profiling, as a Panopticon, corrects and controls individuals' behaviour without allowing individuals to freely exercise control over their data in order to make their own autonomous decisions and choices. It is, therefore, my opinion that the exercise of control should be left to the legislator rather than to the individuals themselves. Profiling constitutes a humanitarian issue and must be governed within the sphere of humanitarian law, as a stand-alone law of profiling in combination with fundamental human rights-based law.

Introduction

Background

Today every individual using the Internet is marked by an immovable electronic *etiquette* which is growing bigger and bigger with every click of the mouse, every email they send, every website they enter, every 'like' or comment they make, every photo they post and every link they share. As a result, this new digital-based lifestyle has increased the level and variety of data generated by each individual (data subject) globally. Most of this information is considered to be personal to the individual and thus extremely private. At the same time, however, such information has become an asset and a valuable tool for both the private and the public sector. Collecting, aggregating and analysing the data of current and potential customers or potential criminal aspects alike enables business and governmental entities (controllers) to discover valuable knowledge about individuals either as customers or as citizens.

Both business and governmental entities increasingly use sophisticated machines that enable the collection and processing of a large amount of data from a number of data sources. These kinds of machines can recognise, locate and identify data, and together with the application of computerised techniques, are able to evaluate and categorise the data into certain groups. The collection of data mostly depends on real-time observation and examination of the data by those machines. As a result, the free flow of data and the (re-) use of data not only take place within the EU borders but also extend globally. Today, business and governmental entities are increasingly moving in the direction of profiling practices.

In the twenty-first century, profiling and its related automated decision-makings constitute a *sovereign* role in almost all business and economic activities, as well as in governments' investigations for the benefit of public safety and national security. Almost everybody in the world accesses the Internet daily, either for personal or business use. As a result, individuals' images and personal

details are constantly recorded by surveillance cameras, security systems, and a number of other sophisticated devices.

What makes profiling practices powerful and beneficial is the fact that profiling results in the automatic categorisation and identification of individuals. It enables business and governmental entities to analyse and predict people's personalities and behaviour (i.e. their social characteristics, their habits, their interests, their economic situation etc.). Profiling can be used in different contexts in our lives and for different purposes. It can be used for security reasons, for marketing purposes, for employment opportunities, for better health treatment, for effective education or for the detection of fraud in the financial sector.

Problem Statement

Profiling, however, brings with it serious concerns of legal, economic, social, psychological and political nature. Individuals are constantly tracked through profiling technologies and different types of information can be merged to link to individuals' physical (offline) lives. Consequently, profiling practices create serious threats to the protection of personal data and the respect of the individual's right to privacy. Both these rights are necessary instruments for a democratic society. Privacy underpins human dignity and other key values of human life and has become one of the most important human rights of the modern age. Personal data refers to any kind of information that can be used to identify an individual, either directly or indirectly, using a combination of different information.

In using profiling technologies to collect, process, store and/or disseminate data, every business entity must comply with data protection legislation. Until recently, the major legislative instrument for data protection in Europe was the Data Protection Directive 96/45/EC (DPD).[1] However, new technological developments have created new legal challenges for data protection legislation that go beyond the

[1] Directive 95/46/EC of the European Parliament and of the Council of October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23/11/1995 P. 0031-0050.

ones considered under the DPD. Therefore, in January 2012, the European Commission drafted the General Data Protection Regulation ('GDPR' or the 'Regulation') which has been applied directly to all Member States since 25th May 2018.[2] The GDPR aims to modernise the current EU data protection legislation and to provide stronger, consistent and uniform rules for the protection of individuals' personal data and for the development of the Internal Market.[3]

Data protection legislation has always been approached within the notion of transparency. This is why data protection legislation does not prohibit processing of personal data but regulates it. In this way, the law tries to defend personal data while, at the same time, it protects the legitimate interest of controllers in processing such data for social and economic purposes. Although the law infers, on the one hand, that the controllers need to be able to process data for their purposes and, on the other hand, that individuals must be able to exercise control over their data, in practice the application of the law may lack certainty and problems may arise with the transparency and accountability of the controllers as well as the effectiveness of individuals' abilities to exercise control over their data. It is questionable, therefore, to what extent it is possible to guarantee protection of individuals' fundamental rights to privacy and data protection within a profiling-based society and whether a mere control, by way of consent, is adequate to provide protection for such rights.

Purpose of the Research

Bearing in mind the above considerations, the research examines the triangle between profiling as a processing activity, the GDPR and the protection of fundamental rights and freedoms, and in particular the rights to privacy and data protection, as well as the related challenges, in order to answer the following main research question:

---

[2] 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, and Repealing Directive 95/46/EC (General Data Protection Regulation).

[3] Peter Hustinx, 'EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation' (1–12 July 2013) Collected Courses of the European University Institute's Academy of European Law, 24th Session on European Union Law <https://secure.edps.europa.eu/EDPSWEB/edps/EDPS/Publications/SpeechArticle/SA2014> (accessed 05 October 2015).

Does the transparent and self-determinatory (controllable) nature of data protection law safeguard the protection of the fundamental rights and freedoms of individuals, especially the rights to privacy and data protection in today's profiling-based society?

Specifically, the research examines the resultant developments on the protection of individuals in relation to profiling emanating from the new EU data protection legal framework. The research is a significant step in identifying and analysing, from a profiling point of view, a number of strengths and weaknesses associated with the new GDPR as well as with the transparent nature of EU data protection legislation in general. It will address whether there is a need for a new class of protection to accommodate this profiling-based environment. Finally, the ideas that will be presented will provide some food for thought on how to improve data protection legislation and how to limit the complexities of European policy-making in order to provide better and more objective safeguards for individuals and their rights within the context of profiling.

Limitations in the Scope of the Thesis

It should be noted that the scope of this thesis is limited to profiling practices operating in the private sector for commercial purposes. This is, firstly, because the main applications of profiling are concerned with the commercial domain (e.g. personalised advertising and pricing, credit scoring practices etc.) and, secondly, because the issues that arise in relation to governments and the law enforcement sector are different and need separate analysis.[4] For the purpose of this thesis, therefore, the terms 'business entities' and 'controller' both refer to any kind of service providers such as bankers, insurance companies, retailers, doctors, universities and so on.

[4] Mireille Hildebrandt, 'Preface' in Niklas Creemers, Daniel Guagnin and Bert-Jaap Koops (eds), *Profiling Technologies in Practice: Applications and Impact on Fundamental Rights and Values* (Wolf Legal Publishers 2015) 2.

Although profiling practices constitute a threat to a number of fundamental rights of individuals, the scope of the present thesis is to address the threats that arise from the processing of data with profiling to the right to privacy and the right to the protection of personal data which are perhaps the most seriously challenged.

Definition of Terms

It is important to clarify the meanings of the different actors which are involved in data processing for profiling purposes. For data to be processed, data controllers must collect information from data subjects. According to the EU data protection law, a *data controller* or *controller* is 'the natural or legal person, public authority, agency or any other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law'.[5] For the purpose of this thesis, a controller refers to a person or a business entity who determines the processing of data for the creation and application of a profile.

The *data subject* is also defined by the EU law as the 'identified or identifiable natural person (…) who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person'.[6] For this thesis, a data subject is the subject (an individual or a group) of the data being processed to create a profile as well as the subject (an individual or a group) to whom the profile applies.[7]

[5] Article 4(7) GDPR.
[6] Article 4(1) GDPR.
[7] It should be noted that, as it will be seen in Chapter 1, the subject from whom the data is collected to create a profile and the subject to whom the profile applies may not be the same in all cases (this is the case of non-distributive group profiling).

In addition, there are other definitions that are not included in the law but are common in the EU context such as the data user. A *data user* or *user* is defined in academic literature as the profiled data subject using a certain machine (e.g. computerised device) that facilitates the recording, storing and processing of data for the controller.[8]

Research Methodology

Since this thesis is textual and qualitative in its methodology, the materials presented are sources from an extensive study of the available literature as well as contacts with legal and technological experts. In particular, the thesis makes extensive use of primary sources, such as legislation, and other secondary material, like journals and textbooks, from libraries in the United Kingdom, Cyprus and the Internet. In order to lay out the general theoretical and philosophical background, the existing scholarly writings and jurisprudence are used as well as relevant European legislation.

The principal legal framework for this research is the General Data Protection Regulation which came into force on 25th May 2018. To describe, identify and analyse the content of the Regulation, the thesis uses a doctrinal approach to the research, which is classical legal research. For the interpretation of the provisions of the GDPR, the thesis refers to the preamble of the Regulation as well as to the case law and the opinions of the Article 29 Working Party that concern the interpretation of the provisions of the DPD. Thus, insofar as the provisions of the Regulation are similar to those of the DPD, the case law or other literature interpretation given for the DPD is used to interpret these provisions.

For the normative part of the thesis, the research uses an extensive range of different normative theories in order to identify, explain and analyse various issues in the research from a descriptive and critical point of view. Additionally, throughout the

[8] Mireille Hildebrandt and James Backhouse, 'D7.2: Descriptive Analysis and Inventor of Profiling Practices' (2005) FIDIS consortium <http://www.fidis.net/resources/deliverables/profiling/> (accessed 14 July 2014) 12.

thesis, many examples are utilised to give better understanding of the subject and to illustrate various points that were important for the research. To examine the effectiveness of the GDPR to adequately protect individuals in the context of profiling, the legal and technological issues of the research are combined. At the end, the findings of all the chapters are combined to answer the research question.

It should be noted that, although profiling has global application, this thesis has taken a European perspective on the subject. This does not mean that the thesis is of interest to EU readers only. Many of the issues discussed in the thesis have an international application and are valid globally, especially since the adoption of the GDPR under which the territorial scope of the Regulation is extended to also cover business entities outside of the EU, if they offer goods and services to EU citizens or if they monitor the behaviour of EU citizens.

Significance of the Research

This thesis is addressed to the legal society and to any other community who may be interested in the subject. The findings of this thesis will contribute to the development of better and more effective protection for individuals, as well as preserving freedom and ensuring democracy in a digital era. In addition, the thesis aims to facilitate further research for safeguarding the protection of the fundamental human rights of individuals, especially the rights to privacy and data protection in today's profiling-based society.

Thesis Contribution to New Knowledge

The present PhD thesis aims to examine the triangle between profiling as a processing activity, the GDPR and the protection of fundamental rights and freedoms, in particular the rights to privacy and data protection, as well as the related challenges. From an EU perspective, the current state of knowledge on the subject of profiling consists of a limited number of primary and secondary sources in this area. Although there are a substantial amount of publications in literature and the business

world about big data analytics and data mining techniques (a step in the profiling process), there are limited publications specifically on profiling, and hence the present research will add that. Below, it is to be argued how the present thesis contributes to a significant new knowledge in the subject of profiling.

This thesis examines the new EU data protection framework as it is adopted under the GDPR. In particular, the thesis evaluates the outcome of the GDPR in relation to profiling and its challenges to individuals' fundamental rights and freedoms as well as to society and thus to democracy. This thesis contributes to new knowledge because from its findings the following arguments have been revealed:

Firstly, it is to be argued that the GDPR, in practice, is insufficient to safeguard the protection of individuals' rights to privacy and data protection within the context of profiling. The application of data protection principles and of the GDPR is not objective in the context of profiling. The distribution of powers is at the expense of individuals and in favour of controllers, both in terms of knowledge and in terms of power, and thus of how they exercise that power.

Secondly, it is to be argued that the GDPR is not intended to restrict profiling activities but rather to offer ways to enable further profiling. As revealed in the findings of Chapter 4, the GDPR gives authorisation to business entities to re-process data for profiling, for any other purposes and without restrictions, by simply claiming the exception of statistical purpose. This is because processing of data for profiling can form processing for statistical purposes under the GDPR since, as it is proven, the definition of *statistics* coincides with the meaning of profiling and the six steps of the Knowledge Discovery in Databases (KDD) process. Thus, any further profiling activity can fall within the exception of statistical purposes of the GDPR and thus be considered to be compatible and lawful with the initial purpose of profiling. In addition, the GDPR encourages business entities to retain data beyond the initial period and (re-) use these data for their future profiling activities. Considering, however, the capacity of profiling to store large amounts of data with almost no cost, the flexibility of further retention may lead controllers to keep the data forever. Furthermore, as it is revealed from the analysis in Chapter 5, the

principle of data minimisation is inconsistent with profiling because, for a profile to be accurate, the controller must collect as many data as possible about the individual subject. By contrast, data minimisation requires the collection, processing and retention of data to what is strictly relevant and necessary for the purposes for which they are collected. However, as it is seen, the controller cannot assess which data will be relevant for a certain profiling because the purposes of the profiling are unforeseeable at the time of the collection of the data.

Thirdly, consent is proved to be a pseudo-right under which the individuals do not have the choice to refuse to give their data or to withdraw their consent without being rejected by the required service or product. Therefore, individuals, in giving their consent, act mechanically and unconsciously due to fear of losing the service. Such consent cannot be considered as the freely given, specific, informed and unambiguous indication of the individuals' wishes.

Fourthly, it is to be argued that the way profiling works interferes with individuals' autonomy and self-determination. Profiling, by nature, creates knowledge asymmetries which result in unbalanced distribution of powers between individuals and business entities. This means limited knowledge and lack of awareness on the part of the individual which undoubtedly results in limited control over their data. In addition, profiling forces people to live according to their past by inferring knowledge based on their previous behaviour and choices. In this way, profiling by its functioning nature reduces the capacity of individuals to freely exercise control over their lives.

Fifthly, it is to be argued that profiling encourages loss of control and separation from the real self. Instead of acting as an individual, a person is experiencing lack of self-awareness, loss of individuality and personal responsibility and loss of self-regulation. This means that the person has lost his/her identity and personality and has become vulnerable to external conditions (the opinions and behaviours of others). More importantly, the lack of self-regulation makes the individual lose control and any sense of control over him/herself and thus over his/her actions.

Further, the individual is neither aware nor able to be aware that he/she is in a situation of lack of knowledge and self-regulation.

Sixthly, from the findings of this thesis it is arguable that profiling creates a situation of panoptic surveillance under which the resulting distribution of powers may lead to social control, social sorting and normalisation of the population. Panopticon is a form of social control by public and private actors. Thus, profiling works as a control mechanism to tempt individuals to adapt their behaviour in order to meet the expectations and beliefs of their profilers. It corrects and controls individuals' behaviour without allowing individuals to freely exercise control over their data in order to make their own autonomous decisions and choices.

Seventhly, the findings of the present thesis reveal that profiling contradicts the idea of transparency and the self-determinatory nature of data protection legislation and thus of the GDPR. This means that profiling is inconsistent with the idea of control and responsibility on the part of the individuals and thus of consent as a control mechanism under the GDPR. Therefore, it is argued that a law of controllable and self-determinatory nature cannot be effective in protecting individuals and ensuring their rights, if individuals themselves have no interest in exercising such control or to live an existence of self-determine.

Structure of the Thesis

The structure of this thesis is organised as follows: Chapter 1 introduces the concept of profiling in order to obtain an understanding of the creation and application of profiles. In doing so, the chapter provides an in-depth description and explanation of profiling along with its technical aspects and its uses in the different fields of its applications. Explaining how profiling works is essential to understand how data are collected and processed by business entities and how they become valuable knowledge about individuals.

Chapter 2 explores the possible challenges that arise from the use of profiling in order to determine how and to what extent individuals are affected by the creation of

profiles and the decisions made based on those profiles. This formulation helps to understand how concerns about the protection of fundamental rights and values of individuals are related to profiling and how profiling can occupy such deep and serious legal emotions.

Chapter 3 presents an overview of the EU data protection legal framework in order to understand the importance of privacy and data protection as it derives from the fundamental values that both rights aim to protect, how the law protects the rights to privacy and data protection as well as to determine the risks and perils that the law intends to prevent. In this respect, the chapter deals with the principles of a democratic constitutional state, the tools of transparency and opacity, the genesis of data protection legislation, the distinction of privacy and data protection as fundamental rights, the EU Data Protection Directive 95/46/EC and the General Data Protection Regulation.

Chapter 4 examines how profiling is regulated in order to determine how the EU law deals with profiling and its challenges to the fundamental rights and values of individuals, notably to the rights to privacy and data protection. In particular, the chapter examines the scope of the application of the Regulation, the general principles for the processing of personal data and the specific provisions regulating profiling.

Chapter 5 combines the findings from previous chapters in order to identify possible problems with the GDPR and to answer the main research question of the thesis. In particular, the chapter examines whether, in practice, there is a balance between profiling and human rights protection under the GDPR, and moreover, whether the protection provided under the Regulation is adequate and effective to ensure the fundamental rights and values of individuals, notably their rights to privacy and data protection, within the context of profiling.

Chapter 1

The Concept of Profiling

1.1. Introduction

The classification of individuals into certain categories and automated decision-making are the trends in today's digital-based society. Today, more and more retailers, bankers, insurers, employers, publishers, doctors and public service providers are all making increasing use of profiling practices. Profiling is a defining challenge of our time. It has introduced new ways for controllers to collect, store, analyse and (re-) use the information (personal and non-personal) of data subjects and thus influence the way business entities interact with individuals' data.

The emergence of these developments is the result of the use of new data-gathering devices (e.g. computers, smart phones, video and audio surveillance, security cameras, GPS, sensors, biometric access devices, credit card payment systems, drones, facial recognition technology etc.),[9] which has contributed to the digitisation of individuals' everyday activities and thus increased the volume of data and the variety of data sources related to each individual.[10] Never before has data about individuals been available to be collected and (re-) used with almost no effort.

Due to these devices – profiling technologies – data can be easily tracked, accumulated and combined from a number of different data sources (e.g. social network profiles, medical records, bank or insurance forms, website tracking information etc.) and together with the application of computerised techniques (data mining techniques),[11] can be automatically evaluated and categorised into certain data groups. Moreover,

[9] Gary T. Marx, 'What's New About the "New Surveillance"? Classifying for Change and Continuity' (2002) 1(1) Surveillance & Society 9.
[10] Corien Prins, 'Averse from Hair-splitting: A Process-based Framework to Balance Privacy and Other Interests' in Hielke Hijmans and Herke Kranenborg (eds), *Data Protection Anno 2014: How to Restore Trust? Peter Hustinx, European Data Protection Supervisor* (2004–2014) (Cambridge: Intersentia Publishing Ltd. 2014) 26; See also Kieron O' Hara and Nigel Shadbolt (ed), *The Spy in the Coffee Machine* (Oneworld Publications 2008) preface vii.
[11] Daniel J. Solove (ed), *The Digital Person* (New York University 2004) 44.

meaningless or incomplete data can be merged with other data and give access to additional data related to individuals.[12]

All these data, generally referred to as 'big data', generate potentials for business entities to create detailed digital records – profiles – of individuals' behaviour, characteristics and activities.[13] The resulting profiles contain, for example, information regarding individuals' physical, demographic (i.e. age, sex, religion, profession, income, education level, marital status etc.), psychographic (i.e. lifestyle, activities, choices, opinions, interests or hobbies, political beliefs, website visits etc.) and geographic (i.e. city or country, location of work or residence etc.) characteristics.[14] These profiles enable business entities to obtain knowledge – patterns of behaviour – about individuals that they would have been unable to obtain otherwise (e.g. information about their private, social or economic life etc.).

Based on these findings (profiles), business entities have the ability to understand the personal needs and preferences of their customers. As such, they can customise their products and services to meet the specific requirements of each individual customer, as well as make decisions in order to build their business models, improve their services and increase their profits.

What makes profiling practices, therefore, powerful and beneficial is the fact that profiling results in the automatic categorisation and identification of individuals. It enables business entities to analyse and predict individuals' personalities and behaviour (i.e. their social characteristics, their habits, their interests, their economic situation etc.) in order that decisions about them can be made accordingly.[15]

---

[12] Solove (ed) 2004 (n 11) 44.
[13] Francesca Bosco et al., 'Profiling Technologies and Fundamental Rights: An Introduction' in Niklas Creemers et al. (eds), *Profiling Technologies in Practice: Applications and Impact on Fundamental Rights and Values* (Wolf Legal Publishers 2015) 5; See also Solove (ed) 2004 (n 11) 3.
[14] Mike Woodworth and Stephen Porter, 'Historical Foundations and Current Applications of Criminal Profiling in Violent Crime Investigations' (1999) 7(4) Expert Evidence 24; See also Solove (ed) 2004 (n 11) 2–4.
[15] Information Commissioner's Office (ICO), 'Big Data and Data Protection 20140728 version: 1.0' (2014) <https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2016/11/big-data-and-data-protection.pdf> (accessed 1 July 2018).

This first chapter introduces the concept of profiling in today's digital era. In doing so, the chapter provides an in-depth description and explanation of profiling along with its technical aspects and its uses in the different fields of its applications. Explaining how profiling works is essential to understand how data is collected and processed by business entities and how it becomes valuable knowledge about individuals. Such knowledge can be a powerful instrument and creates a number of possibilities for business entities to serve their purposes.

In particular, section 1.2 of the chapter provides various definitions for profiling, from academic literature and the legal world, in an attempt to explore and understand its meaning. Section 1.3 provides background to the origins and nature of profiling in order to understand how ideas about profiling have developed over the years. Section 1.4 presents the different forms of profiling. Section 1.5 explains how the visions of Ambient Intelligence (AmI) and Internet of Things (IoT) work in order to understand the extent of the use and application of autonomic profiling in individuals' everyday lives. Section 1.6 examines profiling as: (a) technique, technology and practice, (b) probabilistic knowledge and (c) hypothesis. Section 1.7 illustrates the vital distinctions between the different types of profiles: (a) individual and group profiles, (b) distributive and non-distributive profiles, (c) direct and indirect profiles. Section 1.8 describes the technical process of Knowledge Discovery in Databases (KDD) in order to better understand the way automated profiling works and how it produces knowledge. The analysis of the KDD process is extended by detailed analysis of data mining techniques and the distinction between descriptive and predictive data modelling. This section also explains the role of big data in profiling practices. Section 1.9 investigates the role of different types of technologies through the specific applications of Behavioural, Biometric and Location-Based profiling. Section 1.10 deals with the different purposes and applications of profiling in the private sector.

1.2. Defining Profiling

Profiling is a very complex issue with diverse meanings and applications. In the dictionary, *profiling* is defined as 'the recording and analysis of a person's psychological and behavioural characteristics, so as to assess or predict their

capabilities in a certain sphere or to assist in identifying categories of people'.[16] In the world of academic literature, one of the early definitions of profiling is that given by Gary T. Marx in 1984. When speaking about profiling in the law enforcement sector, Marx described profiling as a method that is characterised by an 'inductive logic' in order to predict probable patterns of behaviour.[17] This means that the data analysed to produce the knowledge are related to the data of numerous individuals with similar behavioural characteristics and not to one specific individual. Specifically, Marx defines profiling as a method that 'permits investigators to correlate a number of distinct data items in order to assess how close a person or event comes to a predetermined characterization or model of infraction'.[18]

Subsequently, Roger Clarke also offered a definition for profiling. Clarke first introduced profiling as a 'dataveillance technique' which involves the 'systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons'.[19] According to him, there are two types of dataveillance technique: 'personal dataveillance' which involves the monitoring of a single person, and 'mass dataveillance' where the monitoring involves a group of people in order to identify individuals within the group.[20] This definition clearly considers profiling as a technique that monitors individuals through their data in order to create a profile for a specific person or group of persons. However, due to the extensive use of profiling for different purposes, Clarke gave another definition to cover all the contexts of its application. He also defined profiling as 'a technique whereby a set of characteristics of a particular class of person is inferred from past experience, and data-holdings are then searched for individuals with a close fit to that set of characteristics'.[21]

In more recent years, a more comprehensive definition of profiling is given by Mireille Hildebrandt: '[t]he process of 'discovering' correlations between data in databases that

[16] Oxford Dictionary Online <https://en.oxforddictionaries.com/definition/profiling> (accessed 2 March 2018).
[17] Gary Marx and Nancy Reichman, 'Routinizing the Discovery of Secrets: Computers as Informants' (1984) 27(4) American Behavioral Scientists 423.
[18] Marx and Reichman 1984 (n 17) 423–452.
[19] Roger A. Clarke, 'Profiling: A Hidden Challenge to the Regulation of Data Surveillance' (1993) 26 Journal of Law, Information and Science 405.
[20] Roger A. Clarke, 'A Normative Regulatory Framework for Computer Matching' (1995) 13 Journal of Computer and Information Law 587.
[21] Clarke 1993 (n 19) 403.

can be used to identify and represent a human or nonhuman subject (individual or group) and/or the application of profiles (sets of correlated data) to individuate and represent a subject or to identify a subject as a member of a group or category'.[22] This definition reflects the general understanding of what profiling is: profiling is the process of creating and applying a profile to an individual or a group of individuals through the analysis and interpretation of data.[23]

Likewise, a more recent definition is that given by Francesca Bosco et al. in the article 'Profiling Technologies and Fundamental Rights. An Introduction': '[p]rofiling is a technique of (partly) automated processing of personal data and/or non-personal data, aimed at producing knowledge by inferring correlations from data in the form of profiles that can subsequently be applied as a basis for decision-makings'.[24] This definition highlights that the data used to create the profiles are not necessarily personal, and that the application of profiles consists of decision-makings upon the individual subjects.

Bearing in mind the above definitions, it is clear that a number of issues are relevant to describe profiling. The main objective of all the definitions is to discover behavioural patterns from the analysis of the available data. This knowledge is used for certain purposes in different contexts. In addition, profiling is defined as a process of constructing a profile, using techniques and technologies, in order to make decisions concerning individuals.

From a legal point of view, until recently, profiling was the subject of unexpectedly limited legal documentation. This is because there was no authoritative definition of profiling under EU law. EU data protection legislation has not provided a specific definition of the term *profiling* nor has it included reference to the word *profiling*. The DPD only provided rules for the processing of personal data in general (the only

[22] Mireille Hildebrandt, 'Defining Profiling: A New Type of Knowledge?' in Mireille Hildebrandt and Serge Gutwirth (eds), *Profiling the European Citizen: Cross-Disciplinary Perspectives* (Springer 2008).
[23] Mireille Hildebrandt, 'Profiling and the Identity of the European Citizens' in Mireille Hildebrandt and Serge Gutwirth (eds), *Profiling the European Citizen: Cross-Disciplinary Perspectives* (Springer Science+Business Media 2008) 303–343.
[24] Francesca Bosco et al., 'National Data Protection Authorities' views on Profiling' in Niklas Creemers et al. (eds), *Profiling Technologies in Practice: Applications and Impact on Fundamental Rights and Values* (Wolf Legal Publishers 2015) 22–23.

provision that could be seen to deal with profiling is Article 15 DPD[25]). Profiling, therefore, was considered as another form of personal data processing that should be governed within the general EU rules of processing.[26]

It was not until 2012 that the EU considered adopting an explicit definition for profiling under the draft of the GDPR.[27] Under the official text of the Regulation, profiling is defined as:

> 'any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;'[28]

According to this definition, profiling consists of two elements: (a) the automatic processing of data to evaluate an individual's personal characteristics – the *creation of profiles* – and (b) the analysis or prediction of an individual's characteristics – the *application of profiles*.[29]

1.3. From Old to New Ways of Profiling

This section commences by providing background to the origins and nature of profiling. Its influence on the private sector is then discussed in order to understand how ideas about profiling developed over the years and how automated (machine) profiling advances within the field of technology have proved to be so valuable for business entities.

---

[25] Article 15(1) DPD: 'Member states shall grant the right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability or conduct etc.'
[26] Bosco et al. 2015b (n 24) 22–23.
[27] Proposal for a Regulation 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 (General Data Protection Regulation), COM (2012), 25/01/2012.
[28] Article 4(4) GDPR.
[29] Hildebrandt 2008b (n 23) 303; See also Bosco et al. 2015b (n 24) 22.

It is widely assumed that profiling became apparent in the late 1970s with developments in information technology (IT) and the increasing number of computer databases.[30] Profiling, however, is not a phenomenon that was invented with the technology, intensive data flow and commercial exploitation of the Internet. Historically, scientists and police authorities have utilised different methods to investigate offences and identify criminals based on the analysis of certain personality characteristics that, if present, could facilitate criminal behaviour.[31]

In the late 1400s, for example, Jacob Sprenger and Heinrich Kramer wrote a book named *Malleus Maleficarum (The Hammer of Witches)* on the investigation and elimination of witchcraft.[32] The purpose of the book was to provide guidelines for witch hunters on how to identify and prosecute witches based on a set of specified characteristics. According to these characteristics, witches were most likely to be women over the age of forty, widows and with little or no weight.[33] In addition, female witches could also be targeted due to the language they used (e.g. rough language) or the fact they were self-independent ('self-reliant'), without a male head of the household, or even because they could float in cold water.[34]

Although witch hunting has nothing to do with today's profiling practices, it appears that it was one of the first old-style methods used for creating certain archetypes of human personality by identifying and categorising individuals into groups (e.g. 'witches' and 'non-witches', 'widows' and 'married women' etc.).

Another example is that of phrenology. In the late 1700s, the anatomist Franz Jozeph Gall developed a theory about the structure of the skull (cranium). He argued that there was a connection between the shape of the skull and the shape of the brain. According

[30] Clarke 1995 (n 20) 586; See also Solove (ed) 2004 (n 11) 18.
[31] Serge Gutwirth and Paul De Hert, 'Regulating Profiling in a Democratic Constitutional State' in Mireille Hildebrandt and Serge Gutwirth (eds), *Profiling the European Citizen: Cross-Disciplinary Perspectives* (Springer Science+Business Media 2008) 286; See also Edward E Sampson and Marya Sampson Marthas (eds), *Group Process for the Health Professions* (New York: John Wiley & Sons Inc 1981) 27.
[32] Woodworth and Porter (1999) (n 14) 243.
[33] Angela Michelle Schultz, 'History and Effects of Witchcraft Prejudice and Intolerance on Early Modern Women' (5 April 2017) <https://exemplore.com/wicca-witchcraft/Gender-Bias-in-Witch-hunts> (accessed 25 September 2017).
[34] Schultz (n 33) 2017.

to Gall, studying the shape and size of the skull and the location of the brain could reveal information about an individual's behaviour and personality. He explained that specific areas of the brain correspond to different mental abilities, tendencies and feelings of individuals.[35]

Gall asserted that the brain consists of twenty-seven different phrenological organs and faculties and that each controls a specific tendency or ability (e.g. faculty of language, ambition and vanity, sense of sounds and musical talent etc.).[36] In other words, he considered the brain as an index of the individual's mental and emotional capabilities. Gall's theory also contained a criminality organ (i.e. 'murder, carnivorousness') which reflected the individual's tendency to behave in a criminal way.[37] Basically, he suggested that a criminal can be identified by the physical characteristics of his/her skull.

In the nineteenth century, an Italian criminologist named Cesare Lombroso introduced another form of criminal profiling based on biological conditions.[38] Lombroso argued that the origins and motivations of criminality are inherited and thus that criminals could be identified by certain biological characteristics of the face as well as by social and psychological factors.[39]

In his book *The Criminal Man* (1876), Lombroso presented the theory of the 'born criminal': that criminals were born with the tendency to offend because of certain biological characteristics.[40] He argued that there were eighteen physical characteristics that could indicate a person as being a born criminal (e.g. too big or too small ears, abnormal teeth, dark skin, too long arms etc.).[41] If five or more of those characteristics were present, a person was identified as a born criminal (atavistic[42] or savage).

---

[35] Frederick Schauer (ed), *Profiles, Probabilities and Stereotypes* (Harvard University Press 2006) 19–21.
[36] Erika Janik, 'The Shape of Your Head and the Shape of Your Mind' (6 January 2014) <https://www.theatlantic.com/health/archive/2014/01/the-shape-of-your-head-and-the-shape-of-your-mind/282578/> (accessed 22 September 2017).
[37] Schauer (ed) 2006 (n 35) 14; See also Roger Cooter, 'The Cultural Meaning of Popular Science: Phrenology and the Organization of Consent in Nineteenth-Century Britain' (Cambridge: University Press 1984).
[38] Woodworth and Porter (1999) (n 14) 244.
[39] Charles A. Ellwood, 'Lombroso's Theory of Crime' (1912) 2(5) Journal of Criminal Law and Criminology 716; See also Gutwirth and Hert (eds) 2008 (n 31) 287.
[40] Ellwood 1912 (n 39) 716–717.
[41] Ellwood 1912 (n 39) 716–723; See also Woodworth and Porter (1999) (n 14) 244.
[42] According to Lombroso, atavistic criminals are those who are not evolved properly.

Following the above, it is obvious that profiling is not a privilege of today's digital era but that its origins stretch back over many decades. In all of the aforesaid theories, the purpose was to create patterns of behaviour (e.g. witches or criminals) by identifying and categorising individuals (e.g. 'criminal' and 'normal' individuals, 'witches' and 'non-witches' etc.) based on their physical, biological, social and psychological conditions. Therefore, these theories constituted a form of profiling which was created in order to identify possible criminal behaviour. The only difference is that today's profiling and data mining practices benefit from the power of technology.

Furthermore, sellers have always utilised different approaches to discover information about their customers based on the analysis of their psychological and demographic characteristics.[43] Such psychological and demographic descriptions could enable better and more precise marketing strategies. In the past, for example, there was a personal relationship between the seller and the customer since they both lived in the same community. Their life together in the community allowed the seller to know various information about the customer. In this way, marketing was done personally in the street or in the shop of the seller.[44]

In the period between the nineteenth and twentieth centuries, personal marketing to known customers was upgraded to mass marketing to anonymous customers.[45] In addition, far more important was the development of targeted marketing, the aim of which was to identify potential customers who were more likely to buy a certain product or service and focus the marketing strategy on them.[46] In this way, sellers could create groups of customers with the same preferences and then decide which marketing approach to follow (e.g. place the advertisement on a particular television programme instead of in a magazine).[47]

[43] Indra Spiecker genannt Döhmann et al., 'The Regulation of Commercial Profiling – A Comparative Analysis' (2016) European Data Protection Law Review 2(4) 535–554.
[44] Solove (ed) 2004 (n 11) 16.
[45] Solove (ed) 2004 (n 11) 16.
[46] Roland Marchand, 'Customer Research as Public Relations: General Motors in the 1930' in Sussan Strasser et al. (eds), *Getting and Spending European and American Consumer Societies in the Twentieth Century* (Washington D.C. Cambridge University Press 1998) 85–86.
[47] Solove (ed) 2004 (n 11) 16.

Furthermore, in the late-nineteenth century, the advent of targeted marketing brought with it the development of direct marketing practices. Direct marketing is a form of targeted advertising in which business entities are advertising directly to their customers. It does not involve, for example, advertising placed on the radio or on the television. The seller communicated directly with potential customers either through mail order catalogues (i.e. sending the catalogues directly to customers), by using doorstep sales (i.e. door-to-door salespersons visiting customers in their homes) or via telephone selling, otherwise known as telemarketing (i.e. calling individuals directly over the phone).[48] Although direct marketing has been a successful practice for business entities, only two percent (2%) of the individuals contacted would respond to purchase the products.[49] Thus, more effective and personalised marketing strategies should be explored in order to meet the preferences of each customer.

By the mid-twentieth century, following the increased volume of data in electronic databases and the use of new technologies, a technique known as computer matching (or data matching)[50] had been developed and was increasingly used in different contexts. Its purpose was to combine data relating to many individuals, from many sources, in order to detect cases of interest (e.g. current or potential criminals or customers).[51] These technological developments gave business entities the opportunity to analyse and categorise individuals' data, in order to make presumptions about their preferences. In this way, targeted marketing technology has evolved. So viewed, with the development of artificial intelligence, the Internet and generally the digitisation of everyday life, the result has been to create a wider situation whereby business entities can use individuals' data to discover information about their customers and become more competitive through this process.

[48] Richard Webber, 'The Evolution of Direct, Data and Digital Marketing' (2013) 14(4) Journal of Direct, Data and Digital Marketing Practices 291–309; See also Solove (ed) 2004 (n 11) 16.
[49] Solove (ed) 2004 (n 11) 17.
[50] The term computer matching was used in the United States and the term data matching was used in Canada, Australia and New Zealand. It should be noted that, while in the countries mentioned above the technique has attracted widespread application, in Europe it has not been widely applied (Clarke 1995 (n 20) 586).
[51] Clarke 1995 (n 20) 586.

1.4. Forms of Machine Profiling

The more advanced the technologies that are available, the more sophisticated the machine profiling will be. This is because a combination of different sets of technologies can lead to autonomous machines which are able to produce real-time analysis and identification of data and thus create profiles of individuals. This section introduces the three forms of machine profiling: non-automated, automated and autonomic profiling.

1.4.1. Non-Automated Profiling

Non-automated profiling involves both the use of a machine and human knowledge. It is the result of collaboration between humans and machines. Its key characteristic is that the construction of a profile does not rely on any process of automatisation despite the use of a machine. Instead, there is a high level of involvement for human expertise in the process. In the case of patients' records, for example, non-automated profiling enables the input of the collected information to a computer. The transfer of information to the computer as well as the categorisation and evaluation of information continue to take place with the doctors' involvement.

1.4.2. Automated Profiling

Automated profiling is the most common type of profiling today. Its development is related to the massive availability of computer systems and the growth of online activities which have increased the size of data in the databases. Automated profiling introduced a new type of knowledge construction resulting from those databases. It is based on the automatic collection and aggregation of data and the discovery of knowledge by the data mining techniques in order to enable human experts to intervene and filter the results in order to make the decisions. Although it replaces, to a large extent, the human involvement in the process, it does not eliminate the need for human intervention in the decision-making process. The procedure is partly automated work and partly human work. For example, a beauty store is collecting information about the

buying preferences of its customers (brands, products, prices etc.) in order to create their profiles – automated action – and, based on these profiles, the beauty store decides to offer them a discount coupon for the skin care products of their favourite brand (human's decision).

1.4.3. Autonomic Profiling

Autonomic profiling is a more self-supported type of profiling.[52] The need for human intervention is eliminated and the decision process is entirely undertaken by the machine. In other words, the machine collects and processes data, creates profiles and makes decisions based on those profiles without human supervision. In online dating applications (e.g. Tinder, OkCupid), for example, based on the results of the users' profiles, the machine will decide which people will be recommended to each user for dating, without the involvement of the service provider. The provider does not have the possibility to see all the users and make a suggestion for each and every one, but the machine makes the decision for him/her.

Its main objective is to create 'a network that is capable of self-management'[53] and therefore accomplish the visions of AmI and the IoT. The visions of AmI and IoT are to bring intelligence into our everyday lives by allowing network devices, which are integrated into our environment, to recognise our presence and to adjust according to our needs, behaviour and environment.

The focus of this thesis is related mostly to automated profiling. Before introducing the main characteristics of machine profiling it is essential, however, to understand the visions of AmI and IoT and therefore the extent of the application of autonomic profiling in individuals' lives.

[52] Mireille Hildebrandt, 'Profiling: From Data to Knowledge' (2006) 30(9) Datenschutz und Datensicherheit (DuD) 550.
[53] Hildebrandt 2008a (n 22) 28.

1.5. Ambient Intelligence and Internet of Things

AmI is a network computing environment that consists of smart devices (i.e. devices with RFID-tags, like TVs, coffee machines, tables, chairs etc.) which are integrated into a person's environment and can recognise his/her presence and be adjusted according to his/her needs and behaviour.[54] Those devices send and receive information about him/her and interpret his/her behaviour (e.g. facial expressions and bodily motions) in order to adjust accordingly.[55]

The idea of AmI is to improve the quality of everyday life by ensuring that the environment treats individuals according to their preferences in a certain context (e.g. smart house, smart restaurant etc.).[56] For instance, a person is driving in his/her car and the radio plays a song that he/she does not like. If the radio recognises by his/her facial expression that he/she does not like the song which is on at that moment, it will automatically switch to another radio station. Such guesswork is the result of the continuous collection of an individual's data (music preference) by the radio which enables the interpretation of the individual's behaviour (e.g. facial expressions and bodily motions) and the adjustment of the radio to the real-time preference of the individual.[57] That is to say, an AmI environment is entitled to foresee individuals' wishes and actions, even before they become aware of them.[58]

Autonomic profiling is, therefore, a valuable tool that enables real-time adjustments to take place by monitoring and collecting data related to individuals' daily (online and offline) activities that will automatically be categorised and profiled. The data collected by these activities will only become valuable knowledge when profiling technologies are applied. Such technologies compose the RFID systems (which allow online

[54] Mireille Hildebrandt, 'Profiling and Rule of Law' (2008) 1(1) Identity in the Information Society (IDIS) 60.
[55] Wim Schreurs et al., 'Report on actual and possible profiling techniques in the field of ambient intelligence, FIDIS (Future of Identity in the Information Society)' (2005) FIDIS Deliverable D7.3 <http://www.fidis.net> (accessed 3 July 2018).
[56] Schreurs et al. 2005, FIDIS Deliverable D7.3 (n 55).
[57] Mireille Hildebrandt, 'Technology and the End of Law' (2009) in Bert Keirsbilck, Wouter Devroe and Erik Claes (eds), *Facing the Limits of the Law* (Springer 2009) 443; See also Mireille Hildebrandt, 'Profiles and Correlatable Humans' in Nico Stehr and Bernd Weiler (eds), *Who Owns Knowledge?* (Transaction Books 2006).
[58] Hildebrandt 2006a (n 52) 550.

activities to be stored and located) and CCTV-cameras and sensor devices (which detect movement, temperature and other data) that together create the IoT.[59]

IoT is a network of connected *things*. It intends to connect everything that can be connected in order to 'turn the offline world online'[60]. The idea of IoT encompasses the vision of computer scientist Mark Weizer for 'ubiquitous computing' in 1980.[61] Weizer supported the view that computers will be incorporated everywhere in the environment and that every object will contain a tiny computer.[62] This means that everyday physical objects (e.g. TVs, radios, washing machines, lamps etc.) are connected to the Internet and they have the ability to transfer data online without requiring human intervention.[63]

More simply, all of these IoT devices are able to detect, for example, movements, temperature, facial expressions, sounds and other information about individuals and things. As a result, data are transferred through the network that connect them while at the same time data are stored in different online databases. As such, meaningless data can be combined with data from other sources to produce useful profiles for individuals.

1.6. Main Characteristics of Profiling

This section examines the three main characteristics of profiling in order to understand how it works: (a) technique, technology and practice, (b) probabilistic knowledge and (c) hypothesis.

1.6.1. Profiling as a Technique, Technology and Practice

In technical terms, a profile is a set of correlated data which is created with the use of profiling technologies, the use of algorithms and other techniques in order to identify patterns that allow for the automatic categorisation of individuals from huge sets of data

[59] Hildebrandt 2008c (n 54) 60.
[60] Hildebrandt 2008c (n 54) 60.
[61] Mark Weizer, 'The Computer of the 21st Century' (September 1991) Scientific American 94–104.
[62] Weizer 1991 (n 61) 94–104.
[63] Hildebrandt 2009a (n 57) 443.

aggregated in large databases.[64] In this way, profiling is the process of constructing or applying a profile to an individual or a group. This process is based on automatic processing *techniques* which are made possible by computer *technologies.* Such techniques involve the collection, aggregation, cleansing and mining of data. On the other hand, computer technologies refer to radio-frequency identification (RFID-tags), computers, smart phones, video and audio surveillance, GPS, sensors, biometric access devices and so on.[65]

Therefore, profiling is a combination of hardware (technologies) and software programmes (techniques) that, together with professional experience and training, result in the construction and application of profiles. A good example by which to understand this combination is the use of fingerprints. The attempt to identify a person by the use of fingerprints is both a technique that requires training and a technology involving hardware (ink and cards and/or electronic imaging devices). [66]

Another aspect of profiling is that profiling is also a practice. This means that profiling does not depend only on the automatic analysis of data by machines and software programmes, but also on human knowledge and practice. As Hildebrandt explains, there is 'a specific way of doing things, within specific contexts, with specific purposes'.[67] This indicates that the construction of a profile does not depend on human intelligence, but on statistical analysis of large amounts of data by machines and software programs trained to identify unknown correlations in databases. Interestingly, therefore, the process involves a minimum degree of human intervention. As Tim Mason, the director of Tesco's Clubcard, admitted: 'You have to use intuition and creativity as well as statistical know-how, and you have to hope that you have identified the right things to test'.[68]

At this point it is important to explain that the term 'data mining' refers to a software technique that automatically analyses data from different data sources, by using

[64] Hildebrandt 2008a (n 22) 17.
[65] Marx 2002 (n 9) 9.
[66] Hildebrandt and Backhouse 2005, FIDIS Deliverable D7.2 (n 8) 12.
[67] Hildebrandt and Backhouse 2005, FIDIS Deliverable D7.2 (n 8) 12.
[68] Hildebrandt and Backhouse 2005, FIDIS Deliverable D7.2 (n 8) 13.

algorithms, in order to discover previously unknown relationships (patterns and correlations) within the data so as to find customers with common preferences. A detailed analysis and examples of the application of data mining techniques and the types of technologies used for the collection of data will be discussed further in sections 1.8 and 1.9 of this chapter.

1.6.2. Profiling as a Probabilistic Knowledge

A profile constructed by profiling technologies is defined as 'a set of correlated data that identify and represent a data subject'[69] (a person, a group or a thing). This implies that profiles are not the same as the original data subject that is profiled, but that they only constitute a representation of the original.[70] Profiling, therefore, identifies a data subject only with a degree of probability and not with certainty.[71] More simply, a profile is a *portrait* of the person, group or thing that is profiled, and is revealed by the mining and cleansing of the data based on past behaviour and characteristics. Essentially, those *portraits – profiles* are based on correlations between data that cannot establish causes or reasons for the outcome. They are probabilistic knowledge in the sense that they involve a degree of variation and a chance of multiple possible outcomes. [72] In other words, they predict what will probably happen but they cannot give reasons as to why this will happen (e.g. why a person will show a certain behaviour in the future). That means that if a pattern appears to occur each time certain conditions are met, it is not absolutely certain that it will occur again in the future.[73] Moreover, one thing that is important to note at this stage is that profiles do not describe reality; the identity constructed through the profiling process is not the real identity of the person being profiled.

[69] Hildebrandt and Backhouse 2005, FIDIS Deliverable D7.2 (n 8) 13.
[70] Hildebrandt and Backhouse 2005, FIDIS Deliverable D7.2 (n 8) 13.
[71] Daniel J. Steinbock, 'Data Matching, Data Mining and Due Process' (2005) Georgia Law Review 10–18.
[72] Jean-Marc Dinant, 'The Concepts of Identity and Identifiability: Legal and Technical Deadlocks for Protecting Human Beings in the Information Society?' in Serge Gutwirth et al. (eds), *Reinventing Data Protection?* (Springer Science+Business Media 2009) 113.
[73] Gloria Gonzalez Fuster, Serge Gutwirth and Erika Ellyne, 'Profiling in the European Union: A High-Risk Practice' (2010) 10 INEX Policy Brief 2.

1.6.3. Profiling as a Hypothesis

Following the fact that the knowledge produced by profiling is a probabilistic one, another way to explain profiling is within the context of hypothesis. In general, a hypothesis is a guess or a prediction, based on prior knowledge and examination, for the purpose of further investigation of a particular subject or phenomenon. Otherwise, a hypothesis provides answers to pre-existing questions; it is the inkling of an idea that can become either a theory or a common, realistic expectation.[74] The basic element of a hypothesis is that there is no pre-set outcome. In terms of profiling, however, a hypothesis is the result of the data mining process, where the controller has no concrete or pre-existing questions in mind to answer.[75] In fact, profiling as a hypothesis is neither an examination nor a further investigation of a particular subject or phenomenon. It is the mining of the data that provides the controllers 'with answers to questions they did not know to ask'.[76] Therefore, the key to awakening in the controller the need for answers and further information is the process of discovering correlations (hypotheses) between the databases.

1.7. Types of Profiling

As was stated above, profiling is the process of constructing or applying a profile to a data subject: an individual or a group. Bart Custers defines the profile as 'a property or a collection of properties of an individual or a group of people'.[77] The profile is revealed by the cleansing and mining of the data in order to discover correlations in the data subject's past and current behaviour and characteristics. The correlated data identify or represent a subject either as a single person or as a member of a group or category. Therefore, profiles can be distinguished as individual or group profiles. Some may also use the term 'risk profiles' for both types in order to show that there is some kind of risk associated with the person or the group (e.g. risk of a person not paying

[74] Fuster, Gutwirth and Ellyne 2010 (n 73) 2.
[75] Viktor Mayer-Schonberger and Yann Padova, 'Regime Change? Enabling Big Data Through Europe's New Data Protection Regulation' (2016) XVII The Columbia Science and Technology Law Review 319.
[76] Hildebrandt 2008a (n 22) 18.
[77] Bart Custers, 'Data Dilemmas in the Information Society: Introduction and Overview' in Bart Custers et al. (eds), *Discrimination and Privacy in the Information Society* (Springer, Berlin, Heidelberg 2013) 13.

his/her debts)[78]. Additionally, the group profiles can be distinguished as distributive and non-distributive group profiles, and direct and indirect profiles.[79]

1.7.1. Individual and Group Profiles

An *individual* or *personal profile* identifies and represents a person based on a set of characteristics.[80] The data are collected in connection with one single person and are based on that person's characteristics and behaviour. An individual profile, for example, is the personal profile of Mr 'X' who is 45 years old, divorced, has 2 children and is a lawyer with a mortgage and one credit card. The purpose of individual profiling is either to identify a person within a group or to detect his/her characteristics for various purposes (e.g. recommending dating places for divorced people or supermarket offers for parents).[81]

A *group* or *aggregated profile* identifies and represents a group of people who share one or more common characteristics.[82] For example, people living in a certain area, on average, may have the same ethnicity or chances of getting asthma. Interestingly, a group may consist of either a community – existing group of people – (e.g. members of a specific religion, association or team), or a category of people that have no connection between them but who share one or more common characteristics (e.g. a group of women with black hair and green eyes).[83] In the case of community, profiling applies to discover shared characteristics between the data of the members of a pre-existing community (e.g. eating preferences, educational level, dressing type, etc.) and not to create a group.[84] In the case of category, profiling applies to create a category of people or a certain type of group whose members share certain common characteristics (e.g. correlations may be found between people who live in the same area and have a certain

[78] Custers 2013 (n 77) 13.
[79] Ferraris et al., 'Defining Profiling' (2013) EU Profiling Project Working Paper <http://profiling-project.eu/wp-content/uploads/2013/07/PROFILINGproject_WS1_definition_2607.pdf> (accessed 13 May 2014) 2.
[80] Ferraris et al. 2013a (n 79) 6.
[81] Hildebrandt 2008a (n 22) 35.
[82] Custers 2013 (n 77) 13; See also Ferraris et al. 2013a (n 79) 5.
[83] Bart Custers, 'The Power of Knowledge – Ethical, Legal and Technological Aspects of Data Mining and Group Profiling in Epidemiology' (Wolf Legal Publishers 2004); See also Hildebrandt 2006a (n 52) 549.
[84] Hildebrandt 2008a (n 22) 35.

level of income).[85] Consequently, a group profiling is a set of correlated data that identifies a group or a person as a member of a group. Group profiles can be classified as distributive and non-distributive profiles.

1.7.2. Distributive and Non-Distributive Profiles

A *distributive group profile* is a group where all the members share the same characteristics.[86] This means that 'the attributes that constitute the group are all shared by every member of the group'.[87] For example, a group of plastic surgeons working in the UK forms a distributive profile. The attributes of the group – that all the members are plastic surgeons working in the UK – are also the characteristics of all the members of the group (every member is a plastic surgeon working in the UK). Thus, the profile applies to the group as a whole but also to each single member of the group, separately, in the form of an individual profile.

On the contrary, a *non-distributive group profile* is a group where the members do not share all the characteristics of the group.[88] This is a more common and complicated type of group profile. For example, a group of people with a high risk of depression is profiled according to a list of risk factors (e.g. economic situation, stressful conditions at work, family history of depression, retiring, losing a job etc.). A person may be identified as a member of that group because he/she lost his/her job and has no income, while another person may be identified as a member of that group because he/she is getting divorced. Therefore, a person may constitute a member of this group without having the same characteristics and without sharing all the same characteristics with others in the group. More simply, not all the members in the group are likely to have depression and even if there is such a possibility, it may not be for the same reasons.

Accordingly, non-distributive profiles are probabilistic in the sense that they 'describe the chance that a certain correlation will occur in the future, on the basis of its

[85] Hildebrandt 2008a (n 22) 35.
[86] Ferraris et al. 2013a (n 79) 5.
[87] Hildebrandt and Backhouse 2005, FIDIS Deliverable D7.2 (n 8) 16.
[88] Ferraris et al. 2013a (n 79) 5.

occurrence in the past'.[89] Thus, if the group of people with a high risk of depression indicates that there is a 90% probability that the members of this group will suffer from depression, this does not mean that, in reality, every person in the group has a 90% possibility of suffering from depression.

1.7.3. Direct and Indirect Profiles

A *direct profile* is used to better define a person or to describe his/her preferences and future behaviour. The data are collected from one single person or a group of people and the knowledge produced will only be applied to this specific person or group in order to predict his/her future behaviour.[90] A service provider, for example, using direct profiling to offer personalised services to a customer based exclusively on his/her previous actions (e.g. his/her past purchases). In other words, the profile applies only to that specific customer from whom the data are collected.

In the case of an *indirect profile* the collection of data derives from a 'large population'.[91] The knowledge is based on categorisation and generalisation.[92] The data will produce groups and categories of people with common characteristics and thus allow the identification of individuals based on the characteristics of those pre-existing groups or categories.[93] In other words, the construction of a profile is the result of 'data referring to other subject[s]'.[94] This means that a decision made for a person is based on the behaviour of other people. A good example of indirect profiling is the way that various online providers offer personalised services to their customers by recommending products based on the preferences of other customers.[95] Following that, as the factors of categorisation and generalisation constitute part of the construction

[89] Hildebrandt 2008a (n 22) 22.
[90] Hildebrandt 2008a (n 22) 41.
[91] Hildebrandt 2008a (n 22) 35.
[92] Hildebrandt 2008a (n 22) 43.
[93] Hildebrandt 2008a (n 22) 35.
[94] Ferraris et al. 2013a (n 79) 6.
[95] Amazon, for instance, provides personalised services to its customers by recommending products based on the views or purchases of other people: 'Customers Who Bought this Item also Bought' or 'Customers Who Bought Item in your Basket Also Bought' (Hildebrandt 2008a (n 22) 43).

procedure of indirect profiling, it can be argued that indirect profiling is a less 'reliable'[96] type of profiling with a 'high degree of uncertainty'.[97]

The definitions of direct and indirect profiles help us to better understand the differences between individual and group profiling and how individual and group profiling work. Perhaps the main difference between the two is due to the fact that decisions, in the case of group profiling, are made based on generalisation while the decisions made on individual profiling are based on particularism.[98]

1.8. The Technical Process of Profiling

The capacity of today's computer systems to store and process (personal and non-personal) information has been continually increasing and allowing the collection of massive amounts of data in databases. This increase has made apparent the need for society to find ways to utilise all these available data and turn them into valuable assets for various purposes (e.g. targeted advertising, criminal investigation, employment opportunities etc.).

Historically, the necessary analysis of data was performed by human analysts and the decision-making process relied on the expert knowledge of the analysts. However, with the massive amount of data contained in large databases, the analysis of data by human experts becomes impracticable. Not only because of the time and cost needed to analyse this size of data but also because a single question may produce hundreds or even thousands of results.[99]

In order to achieve a more automated and accurate analysis of the data, new computerised techniques have been developed to assist the automatic construction of profiles and to enable business entities to discover information about data that is impossible to be recognised otherwise. To understand in what ways these

[96] Hildebrandt 2008a (n 22) 43.
[97] Ferraris et al. 2013a (n 79) 6.
[98] Schauer (ed) 2006 (n 35) 19–21.
[99] Usama M. Fayyad, 'Data Mining and Knowledge Discovery: Making Sense Out of Data' (1996) 11(5) IEEE Expert 21.

technological developments have reformed the construction of profiles today, we shall examine the way profiling is related to Knowledge Discovery in Databases and data mining techniques.

1.8.1. Knowledge Discovery in Databases (KDD)

Automated profiling can be described as the process of KDD in which data mining techniques take place. The data mining technique is a step in the KDD procedure that applies mathematical algorithms to discover patterns and correlations in large databases.[100] It is important to mention that the term 'data mining' can also be used as a synonym of KDD to describe the entire process. In this study 'KDD' will refer to the whole process while the term 'data mining' will be used to describe a step in the process (see step 3 below).

KDD is the process of the 'nontrivial extraction of implicit, previously unknown, and potentially useful information from the data'[101] which enables the creation of profiles. The process of KDD involves six steps:

Step 1: Data recording

The first step of the process is the collection of the relevant data by offline or online activities, either by asking for information directly from people or by monitoring people's movements (e.g. with the use of cookies, CCTVs, sensors etc.). The importance of this step is that the data collected 'will serve as input'[102] for the KDD process in order to produce profiles. What is crucial at this stage is that if the collected data are 'incorrect and/or incomplete [they] may impact the construction of profiles by producing false negatives and false positives'.[103] This means that either a person is included in the profile where he/she should not be included (false positive) or a person who should be included in the profile is not included (false negative). For

[100] Bart W. Schermer, 'The Limits of Privacy in Automated Profiling and Data Mining' (2011) 27.
[101] Schermer 2011, (n 100) p. 27.
[102] Hildebrandt and Backhouse 2005, FIDIS Deliverable D7.2, (n 8) p. 23.
[103] Hildebrandt and Backhouse 2005, FIDIS Deliverable D7.2, (n 8) p. 23.

example, a person is found to be a high-risk customer when he/she is not or a person is found to be low-risk customer while he/she is a high-risk customer.

Step 2: Data preparation

The second step refers to the organisation, or warehousing, and cleansing of the data in order to be ready for use. As already mentioned, not all collected data are useful until they are aggregated in a certain way, and stored over a period of time, in order to link data to the same data subject.[104] For instance, a business entity has to recognise a number of activities that link to the same individual in order to identify that individual as a potential customer.

Step 3: Data mining

This is the most important step in the process where the actual work is done by modelling or mining the data in order to create the profile. Data mining is applied to identify useful patterns of behaviour (profiles), or to check if an existing profile fits with the new (aggregated) data.[105] The discovery of patterns and correlations in the data takes place automatically by the use of algorithms (mathematical formulas or models). Following the above example of a potential customer, the resulting patterns will identify a number of activities of a customer.

Step 4: Data interpretation

The fourth step involves the examination and interpretation of the results derived from the mining of the data. In other words, it is the process of explaining the meaning of the results (patterns and correlations) in order for the collected data to start making sense.[106] For example, a business entity will examine the resulting patterns and correlations in order to ensure they are equivalent to a potential customer behaviour.

[104] Hildebrandt and Backhouse 2005, FIDIS Deliverable D7.2 (n 8) 24.
[105] Hildebrandt and Backhouse 2005, FIDIS Deliverable D7.2 (n 8) 24.
[106] Hildebrandt 2006a (n 52) 549.

Step 5: Data evaluation

This step evaluates the usefulness of the profile. After patterns within the correlated data have been identified and interpreted, it is necessary to test the effectiveness of their meaning in order to be certain that they will successfully produce the desired result within a particular context. Basically, the purpose of this step is to examine the 'adequacy of the profiling'.[107] In other words, experts use their professional knowledge to examine the relevance of the results (e.g. whether an individual's activities show behaviour of a potential customer).

Step 6: Application of profiles

This step helps the controller to utilise the knowledge discovered from the construction of the profile in order to make better and more effective decisions for his/her business. Once the profile is evaluated, a data subject can be identified as a member of that profile and decisions are made and actions are taken for the application of the resulting profile. Therefore, the controller will decide how to use the profile and for what purposes.[108] For example, the individual is identified as a potential customer and the business entity will decide how to promote its products to him/her (personalised advertising).

1.8.2. Data Mining

In this section, data mining techniques (Step 3 above) will be further explored in order to better understand their impact on the outcome of the profiling process. As it was already explained above, the data mining techniques are applied to identify patterns and correlations within the data. These patterns and correlations can be described as a data mining model that can produce either descriptive or predictive results. A descriptive result can help controllers to better understand the information used in the process ('what has happened?'). A predictive result, on the other hand,

[107] Hildebrandt and Backhouse 2005, FIDIS Deliverable D7.2 (n 8) 24.
[108] Hildebrandt and Backhouse 2005, FIDIS Deliverable D7.2 (n 8) 26.

generates new information based on the collected data ('what could happen?'). However, there are two models of data mining techniques: *descriptive modelling* and *predictive modelling*.[109]

i. Descriptive Modelling: *'Monitoring of Behaviour'*

Descriptive modelling aims to examine past behaviour (accepted patterns or models) by mining pre-collected data in order to understand how that behaviour might influence future outcomes. Its objective is to identify common characteristics between different data subjects in a database and discover knowledge that will enable controllers to act accordingly for future purposes.[110] Descriptive modelling corresponds with deductive process in the sense that profiling is testing a hypothesis; it fits 'models to a dataset' or 'identif[ies] behaviours [based on] accepted patterns or models of behaviour'.[111] Descriptive modelling can be used, for example, to categorise customers by their product preferences and life stage.

ii. Predictive Modelling: *'Identification of Behaviour'*

In predictive modelling, the aim is to make a prediction about the probable future outcome of an event or the likelihood of a situation occurring by using known information.[112] In this case, the purpose of profiling is to exploit data and uncover patterns or connections between the data that were previously unknown in order to turn those data into useful information.[113] Predictive modelling often uses the method of classification to establish if a data subject fits to a certain group according to the similarities that are shared with the members of the group. It is important to note that predictive modelling only determines the likelihood of a result.[114] There is no statistical algorithm that can predict the future behaviour of a data subject with

[109] Ferraris et al. 2013a (n 79) 7.
[110] Schermer 2011 (n 100) 46.
[111] Ana Canhoto and James Backhouse, 'General Description of the Process of Behavioural Profiling' in Hildebrandt M and Gutwirth S (eds), *Profiling the European Citizen: Cross-Disciplinary Perspectives* (Springer 2008) 49.
[112] Schermer 2011 (n 100) 46.
[113] Schermer 2011 (n 100) 46.
[114] Schermer 2011 (n 100) 46.

100% certainty. Therefore, the outcome of predictive modelling 'will always be of a probabilistic nature'.[115] A common application of predictive modelling is its use for marketing purposes. A customer's gender, age and purchase history might predict the likelihood of a future sale to that customer.

Following the above, both descriptive and predictive modelling constitute key elements in the construction and application of profiling. Even though, in practice, the two models are 'interrelated',[116] there is a considerable difference in the way profiling is used. In the case of descriptive modelling, profiling is used to monitor the behaviour of the data subjects, while in predictive modelling, profiling is used to identify the data subjects' behaviour. As it will be explained below, the identification and monitoring of behaviour are essential elements in the debate surrounding privacy, data protection and profiling.

1.8.3. Big Data

An essential characteristic of profiling practices is big data. Big data is the basic resource of the KDD process and data mining techniques. The term *big data* describes an enormous amount of data that have become available due to the use of new technologies (i.e. RFID, mobile devices, sensors, cameras etc.). It refers to petabytes and exabytes of data that consist of billions or trillions of records of millions of people by different sources.[117]

One of the most common definitions of big data is that given by industry analyst Doug Laney (VP and Distinguished Analyst with Gartner Research). Laney defined big data as containing three elements: *volume* (refers to the enormous amount of data generated and collected by business entities); *velocity* (refers to the speed at which collected data must be analysed); and *variety* (refers to the managing of large

[115] Schermer 2011 (n 100) 46.
[116] Canhoto and Backhouse 2008 (n 111) 49.
[117] Vangie Beal, 'Big Data' (16 June 2015) <http://www.webopedia.com/TERM/B/big_data.html> (accessed 1 June 2018).

volumes of different types of collected data).[118] Given Laney's definition, it is obvious that 'what turns data into big data is the amount of information, and the speed at which it can be created, collected and analysed'.[119]

The big data analysis process, known as 'big data analytics', examines large amounts of data of a variety of data types (text, video, audio, etc.) to uncover unknown patterns, correlations, market trends, customer preferences and other useful information.[120] The primary aim of big data analytics is to enable business entities to improve their services and make better and faster decisions. Arguably, there is a connection between profiling and big data practices. Without the existence and analysis of big data, profiling practices would not be so prosperous and beneficial for controllers. Big data enables profiling to identify, monitor and predict all kinds of behaviour.

1.9. Profiling and Technologies

This section explains how personalised technologies are used as a tool to benefit profiling practices. As it has already been explained in section 1.6.1 above, automated profiling is a combination of techniques and technologies that, together with professional experience (practice), result in the construction and application of profiles. Therefore, profiling is the use of advanced computer technologies that enable the monitoring of individual activities and the collection of sources (data) for the creation of profiles. The significance of profiling technologies is that they allow the tracking of online (e.g. using cookies) and offline (e.g. using RFID-tags) behaviour as well as the substance of the person's body (e.g. using biometrics).[121] This results in the identification of individuals and therefore gives business entities the advantage of being able to provide personalised services. In order to better

[118] Brandon Butler, 'When does 'big data' become big? AWS, IBM and Research Firms Each Have Their Own Definitions' (2012) NetworkWorld <http://www.networkworld.com/article/2188435/data-center/defining--big-data--depends-on-who-s-doing-the-defining.html> accessed 2 July 2014.
[119] Ferraris et al. 2013a (n 79) 9.
[120] Ferraris et al. 2013a (n 79) 9.
[121] Hildebrandt and Backhouse 2005, FIDIS Deliverable D7.2 (n 8) 15.

understand how those technologies work, the importance of their application is examined in the contexts of Behavioural, Biometric and Location-Based profiling.

1.9.1. Behavioural or Online Profiling

Behavioural or online profiling relies on the development of the Internet and its extensive use by web users. Behavioural profiling is commonly used by all kinds of business entities in order to help them gain better knowledge about their *web anonymous customers*. The Internet is a valuable source for profiling and perhaps the only source that can provide a large amount of different data about a single person. Online data refers to the online behaviour of a user and involves every sort of interaction that can take place on the Internet.

Behavioural profiling, therefore, involves the collection and analysis of a customer's online data that can be used to target advertisements and personalise or customise services based on a customer's specific needs. The categorisation of a customer depends on the patterns of behaviour that are revealed by the mining of the data and includes the customer's personal information and the level (e.g. 'is he/she often visiting the website?') and nature (e.g. 'does he/she participate in a discussion or is he/she only a viewer?') of participation in the website.[122] The European Commission defined behavioural profiling as:

> '[A] technique used by online publishers and advertisers to increase the effectiveness of their campaigns (…) by using information collected on an individual's web-browsing behaviour, such as the pages they have visited or the searches they have made, to select which advertisements to display to that individual.'[123]

Personalisation and customisation are useful for marketing and are profit-generating mechanisms for business entities. From a web perspective, personalisation 'can be

[122] Hildebrandt and Backhouse 2005, FIDIS Deliverable D7.2 (n 8) 95–96.

[123] Mathias Vermeulen, (2013) 'Regulating Profiling in the European Data Protection Regulation: An Interim Insight Into the Drafting of Article 20' (EMSOC-IWT-Brussels Leuven Ghent 2013) 6.

described as any action that makes the web experience of a user personalised to the taste of the user'.[124] More simply, business entities take into account the past online behaviour of users and, after applying profiling techniques, offer to the users the products that they will be most likely to buy according to their preferences. Customisation aims to predict changes in customers' preferences and enables the business entities to differentiate their products from other providers in order to ensure that customers remain satisfied. The difference between personalisation and customisation is 'who controls the creation of [a] user profile'.[125] Whereas in customisation the users are in control of the process by disclosing their preferences or needs, in personalisation there is no explicit control over the process.[126] The profile is created automatically by the system 'without the consent or even the awareness'[127] of the users.

There are various technologies used for behavioural profiling such as cookies, device fingerprinting and deep packet inspection technology. These technologies monitor online activities of the users across the Internet and collect, store and analyse data for the creation of users' profiles. The most common application is that of cookies technology. When a user is visiting a website, the website places on the user's computer a cookie that enables the transition of information back to the website's computer.[128] This information concerns the user's activity on the visiting website. Cookies allow a business entity to monitor the user's movements on its website (e.g. what the user has bought) and to know the 'length and time of the visit'.[129] Although tracking is done anonymously, users need to give their permission before a website can place a cookie on their computer.

Of course, the activities of those users who do not accept cookies can also be tracked with the use of session IDs. A session ID is a unique number (e.g. session ID 5234) that the website assigns to the user in order to grant to him/her access to the website.

---

[124] Emmanuel Benoist, 'Collecting Data for the Profiling of Web Users' in Mireille Hildebrandt and Serge Gutwirth (eds), *Profiling the European Citizen: Cross-Disciplinary Perspectives* (Springer 2008) 176.
[125] Bamshad Mobasher, 'Data Mining for Web Personalization' in Peter Brusilovsky, Alfred Kobsa and Wolfgang Nejdl (eds), *The Adaptive Web: Methods and Strategies of Web Personalization* (Springer 2007) 90.
[126] Benoist 2008 (n 124) 176.
[127] Benoist 2008 (n 124) 176.
[128] Thibodeau Patrick, 'Online Profiling' (2000) 34(38) Computerworld 56.
[129] Patrick 2000 (n 128) 56.

The access is only for a session (the duration of a visit). Every time the user enters the website he/she is assigned a new session ID. The session ID allows the creation of a username and password in order to identify the user, as well as the creation of a virtual shopping bag to store all the goods purchased by the user.[130]

Cookies are also used to combine a variety of data from different websites and link the data to the same user despite the fact that a user has different ID on each website.[131] This means that business entities are able to track a user's behaviour on more than one visit and on more than one website. Basically, the tracking takes place the whole time a user is online and not only when visiting a particular website. The idea is to create a trace of the user and to identify the user's computer when accessing the Internet. Following this, the possibilities of threats to privacy and personal data are enormous for the users. Online data can create detailed history records of the user's online behaviour and, when analysed, provide profiles with personally identifiable information that can link to an offline (physical) person.[132]

1.9.2. Biometric Profiling

The application of biometric technology has increased dramatically in recent years. The analysis of biological data has become a valuable source for profiling that can be used for a great number of purposes. Biometrics 'refers to the scientific and technological measurement of either physiological or behavioural human characteristics'.[133] In other words, biometric technology recognises and identifies individuals by analysing their biological characteristics (e.g. facial characteristics, the shape of hands, the length of fingers etc.). Biometric technologies include a variety of systems like scanners, sensors and detectors, smart surveillance camera systems (e.g. CCTV) and recognition systems.

[130] Hildebrandt and Backhouse 2005, FIDIS Deliverable D7.2 (n 8) 37, 78.
[131] Hildebrandt and Backhouse 2005, FIDIS Deliverable D7.2 (n 8) 37.
[132] Patrick 2000 (n 128) 56.
[133] Angelos Yannopoulos, Vassiliki Andronikou and Theodora Varvarigou, 'Behavioural Biometric Profiling' in Mireille Hildebrandt and Serge Gutwirth (eds.), *Profiling the European Citizen: Cross-Disciplinary Perspectives* (Springer 2008) 89.

Biometric identification is considered to be more trustworthy than other types of identification because it is based on the unique biological characteristics of the person.[134] Such characteristics 'cannot be forgotten, lost, shared, broken or stolen (unless surgery takes place)'.[135] There are two main categories of biometrics: *physiological* (or passive) and *behavioural* (or active) biometrics. The former category includes 'fixed or stable human characteristics'[136] (i.e. face image, fingerprints, ear prints, DNA etc.). The latter category concerns the 'measurements of characteristics'[137] represented by an individual's skills, actions or functions that take place at a specific time for a specific purpose (e.g. mouse movement or method of typing). Both categories are used to achieve identification and verification of the individual subject.[138]

From a profiling perspective, verification is an attempt to verify the identity of a known person by comparing new collected data with existing data in the database. Identification, on the other hand, establishes the identity of an unknown person by comparing new data with any data in the database in order to find a match. However, biometric data can either directly characterise a data subject in a profile or link that subject to an existing (non-biometric) profile. By linking an individual to an existing profile, biometric data offers the opportunity to track the activities of that individual on a daily basis.[139]

Bearing in mind that the use of biometric technologies involves the automatic identification and verification of individuals, the application of biometric profiling is an issue of concern for different areas of law and more importantly for data protection legislation.

---

[134] Angelos Yannopoulos, Vassiliki Andronikou and Theodora Varvarigou, 'Biometric Profiling: Opportunities and Risks' in Mireille Hildebrandt and Serge Gutwirth (eds.), *Profiling the European Citizen: Cross-Disciplinary Perspectives* (Springer 2008) 132.
[135] Yannopoulos 2008b (n 134) 132.
[136] Yannopoulos 2008b (n 134) 131.
[137] Yannopoulos 2008b (n 134) 131.
[138] Hildebrandt and Backhouse 2005, FIDIS Deliverable D7.2 (n 8) 39.
[139] Yannopoulos 2008b (n 134) 132.

1.9.3. Location-Based Profiling

Location profiling is related to Location-Based Services (LBS). LBS are information services accessible with mobile devices through mobile networks and they have the ability to locate mobile users geographically and deliver services to the users based on their location. In LBS, profiling is used to discover patterns and correlations within the collected data in order to predict the location of a person. Location data is collected with the use of Location-Based Technology or Location Tracking Technology.[140] Such technology includes RFID systems, smart personal devices (e.g. mobile phones), wireless technology, global positioning systems (e.g. GPS) and geographical information systems (e.g. GIS devices). These technologies are used everywhere and they can track people as well as objects. However, the importance of location profiling is that it can collect data at any time and in any place. For instance, smart phones 'produce data that can be collected from the moment they are switched on' with no possibility to prevent the collection of data unless the phone is switched off.[141]

The principal source of location profiling is the location of the data subject. Like online and biometric data, location data, when analysed, can be linked to a person and disclose information about that person. Location not only reveals information as to that person's geographical position but also provides information as to that person's presence, social status and identity. Nevertheless, location is not a valuable asset by itself unless it is combined with other information. For example, if an LBS finds a person's position two blocks away from a shopping mall, it is good information but it does not reveal much about his/her identity. But, if an LBS finds his/her presence in the shopping mall, this information will enhance the value of the data and thus reveal something about his/her identity (e.g. he/she likes shopping).

[140] Lothar Fritsch, 'Profiling and Location-Based Services (LBS)' in Mireille Hildebrandt and Serge Gutwirth (eds), *Profiling the European Citizen: Cross-Disciplinary Perspectives* (Springer 2008) 147.
[141] Fritsch 2008 (n 140) 163.

According to sociologist Gary Marx, location can be defined as 'a part of human beings''[142] identity. An identity refers to 'any subset of attributes of a person which sufficiently identifies this individual person within any set of persons'.[143] Therefore, identity is not considered to be a single identifier but involves several different attributes of a person.[144] This means that location is only 'a mere attribute of an identity'.[145] Additionally, since the position of a person changes quickly, location is a variable attribute of identity which creates questions as to the accuracy of the data and the 'volatility and stability'[146] of the results of the KDD process.

Location profiling is divided into two types of profiling. The first type is the 'classic profiling'[147] which is based on the KDD process. The data are collected by a 'locatable device'[148] (e.g. mobile phone) and are used to create individual or group profiles. This is the most common application of profiles in LBS. The main feature of this type of profiling is that the location data link to a 'pre-existing profile'[149] in order to be correlated with the patterns (e.g. food preference) already found in that profile (e.g. links patterns with locations).[150] The second type of profiling involves two categories. In the first, profiling is based only on the location data collected, whereas in the second, profiling is based on the combination of location data with other types of data. LBS regularly track the location of a mobile device and analyse those data along with data from other sources to discover information about 'the location' and 'the individual in this location'.[151] In the first category, the amount of information revealed about an individual's behaviour is less than the information discovered in the second category. In either case, information related to location data is considered to be personal data and, together with other sources of data, provides valuable knowledge relating to the behaviour and identity of the mobile users.

---

[142] Gary T. Marx, 'What's in a Name? Some Reflections in the Sociology of Anatomy' (1999) 15(2) Information Society: An International Journal 99.
[143] Andreas Pfitzmann and Marit Hansen, 'Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management – A Consolidated Proposal for Terminology' (2008) <https://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.31.pdf> (accessed 21 April 2015).
[144] Fritsch 2008 (n 140) 148.
[145] Fritsch 2008 (n 140) 148.
[146] Fritsch 2008 (n 140) 148.
[147] Fritsch 2008 (n 140) 161.
[148] Fritsch 2008 (n 140) 161.
[149] Fritsch 2008 (n 140) 161.
[150] Fritsch 2008 (n 140) 161.
[151] Fritsch 2008 (n 140) 161.

1.10. The Purposes of Profiling and the Fields of Application

After analysing the techniques and technologies used for profiling, the purposes of profiling and the different fields of its application are introduced below. As it is mentioned earlier in this chapter, profiling can be used and applied in different contexts of life and for different purposes. It can be used for security reasons, marketing purposes, employment opportunities, better health treatment, effective education or the detection of financial fraud. The purposes of profiling are defined by the 'explicit objectives'[152] of the controller and the field of its application. For example, the motive of a business entity (e.g. to find new customers) is not the same as the motive of a governmental entity (e.g. to detect potential terrorists). Whether for commercial purposes or for security purposes, profiling is applied to predict future behaviour and identify individuals within certain categories.

1.11. Applications in the Private Sector

At this stage, the use of profiling in different fields of application in the private sector will be explored. This includes the following sectors: marketing, financial, health care, employment, education, and finally, the worlds of social media, social networks and the web.

i. Marketing

Profiling in marketing is becoming 'a routine'[153] practice for business entities. It provides unlimited possibilities for companies to discover information about customers' preferences, needs and buying habits by mining customers' data to uncover patterns that enable more effective marketing, reduce cost and increase revenue. What is interesting here is that business entities do not apply profiling only to understand and predict the behaviour of one individual customer, but also to make

[152] Ferraris et al. 2013a (n 79) 19.
[153] Ferraris et al. 2013a (n 79) 28.

a generalised prediction about the behaviour of a particular class of customers.[154] In other words, profiling is used to classify customers into groups based on the prediction of their future behaviour, and thus create new opportunities for the business entities.

Another popular application of profiling in this field is the 'Customer Loyalty Programme' (CLP). A CLP is the result of long-term marketing research and efforts in order to provide rewards (e.g. customer discounts) for customers to encourage their loyal behaviour to the company. In most cases, apart from the necessary data, additional personal data (e.g. date of birth, contact details, information related to personal life, etc.) are collected for the purpose of market research and advertising.[155]

ii. Financial Sector

One of the major applications of profiling practices is in the financial sector. Nowadays, the phenomenon of financial fraud, including credit card fraud and money laundering, is becoming an increasingly serious problem. The implementation of profiling techniques enables the detection of suspicious economic transactions and fraudulent financial behaviour. Profiling techniques have been applied most extensively for anti-money laundering purposes, for prevention of credit card fraud and in the fight against tax evasion.

In the case of anti-money laundering, all financial and legal entities are required to establish procedures to recognise suspicious activities (e.g. financial transfers from criminal activities) and to report those activities to law enforcement agencies for investigation. A common procedure for these purposes is the use of a Suspicious Activity Report (SAR).[156] An SAR is generated by automated monitoring systems usually consisting of algorithms that analyse data and produce models of financial

[154] Hildebrandt and Backhouse 2005, FIDIS Deliverable D7.2 (n 8) 55.
[155] Ferraris et al. 2013a (n 79) 28.
[156] Hildebrandt and Backhouse 2005, FIDIS Deliverable D7.2 (n 8) 57.

behaviour.[157] The problem with these systems is the large number of false positive results. The algorithms are based on the 'right and wrong' approach to build the profiles. This means that the algorithms do not question the results (whether right or wrong) according to each individual case but take the results as given.[158] Another problem with anti-money laundering profiling is the lack of new advanced methods. Thus, the profiles rely on tried and tested money laundering typologies rather than developing new, advanced and modern procedures.

Another example of profiling application is the prevention of credit card fraud. In Germany, for example, banks and other financial entities use profiling to minimise credit card risks. After obtaining customers' consent, they transfer data related to bank accounts and the financial behaviour of German citizens to the SCHUFA.[159] Profiling technologies then analyse the collected data, along with data collected from customers of other banks, and give the scoring value that determines the risk and the conditions under which a customer can obtain a loan, according to his/her past behaviour.[160] Considering the false positive results that may occur and the lack of clarity on the scoring value process, a number of consequences may arise from the application of profiling. For instance, a person may be assigned a low scoring value and as a result not be able to obtain a loan or to open a bank account. Following this, the SCHUFA system is claimed to violate the Federal German Data Protection Act.[161]

Additionally, in the financial sector profiling can be used to detect tax evasion. Using profiling technologies, the tax authorities may filter possible fraudulent tax behaviours and effectively reduce the losses from income tax and VAT evasion acts. For these purposes, the Italian government developed a system called Redditometro to fight tax evasion in Italy.[162] Like SCHUFA, the idea is to collect in one database

[157] Hildebrandt and Backhouse 2005, FIDIS Deliverable D7.2 (n 8) 57.
[158] Hildebrandt and Backhouse 2005, FIDIS Deliverable D7.2 (n 8) 57.
[159] 'Schutzgemeinschaft fur allgemeine Kreditsicherung' (English: Protection Company for General Creditworthiness).
[160] Hildebrandt and Backhouse 2005, FIDIS Deliverable D7.2 (n 8) 57.
[161] Hildebrandt and Backhouse 2005, FIDIS Deliverable D7.2 (n 8) 59.
[162] V. Ferraris, F. Bosco and E. D'Angelo, 'The Impact of Profiling on Fundamental Rights' (2013) EU Profiling Project Working Paper <http://www.unicri.it/special_topics/citizen_profiling/PROFILINGproject_WS1_Fundamental_1110.pdf> (accessed 13 May 2014) 3.

all data concerning Italian taxpayers and create their profiles based on their previous behaviour and activities.[163] Once more, the use of Redditometro creates a number of issues related to lack of clarity and lack of protection of personal data.

iii. HealthCare

Profiling holds great potential for the healthcare industry. Data mining techniques enable health systems to analyse a huge amount of medical data and turn them into useful information for better practices that improve care and reduce costs. For example, profiling practices may apply to evaluate the effectiveness of a treatment, manage customer relationships, support clinicians, detect medical fraud and abuse and provide better and more affordable healthcare services.[164]

Another interesting application in this field is that of 'predictive medicine' or 'personalised medicine'.[165] The data mining techniques enable doctors to predict the patient's health or to determine the likelihood of a successful treatment for a particular patient based on certain characteristics of a certain group. For instance, a doctor can compare the age, diet and lifestyle of a patient with a group of thousands of people with similar characteristics and discover that the patient needs treatment to prevent a stroke.

Although profiling is a very powerful tool for medicine, there are strict limitations on the accessibility of the patients' health records because health data constitute personal data for the patient.

iv. Employment

In employment, profiling is often used for security (e.g. prevention of fraud and unlawful activities) and human resource management purposes (e.g. supervision of employees). In Germany, for example, supermarkets apply profiling to 'detect

[163] Ferraris et al. 2013a (n 79) 26.
[164] Ferraris, Bosco and D'Angelo 2013b (n 162) 12.
[165] Ferraris et al. 2013a (n 79) 26.

possible embezzlement of cashiers'.[166] In order to establish fraudulent behaviour, profiling techniques will examine the frequency of refund transactions carried out by the cashiers. If a higher rate of refund transaction than average is detected, this could imply fraud and profiling identifies the likelihood of a potentially responsible worker.[167]

Employers may also use profiling practices to observe employees' Internet access and email communications in order to prevent unlawful activities within the organisation. For human resource management reasons, business entities use profiling to analyse the interests, potentials and capacities of their employees. Profiling may also be used to help business entities to improve their hiring decisions by looking for patterns in the online behaviour of job candidates. It is important to note that, for security purposes, the type of profiling used is the distributive group profile, while for human resources management purposes the individual type of profile is applied. In any case, employees have the right to be informed of the processing of their personal data and are entitled to object or to challenge the results of such processing.[168]

v. Education

Educational profiling has become increasingly important and very promising for the educational community. The mining and modeling of educational data give the opportunity to schools, universities and researchers to better understand students, improve educational effectiveness and support research and learning. In traditional education, profiling is used to identify the characteristics of a student and to evaluate his/her skills and progress in a particular area. The use of personality or intelligence testing is very popular in order to assess students' 'motivations, desires, learning style, previous experience or personality'.[169]

[166] Ferraris et al. 2013a (n 79) 27.
[167] Hildebrandt and Backhouse 2005, FIDIS Deliverable D7.2 (n 8) 57.
[168] Ferraris et al. 2013a (n 79) 27; See also Ferraris, Bosco and D'Angelo 2013b (n 162) 10.
[169] Hildebrandt and Backhouse 2005, FIDIS Deliverable D7.2 (n 8) 61.

In the world of e-learning, the application of profiling is considered differently. Profiling in e-learning takes two forms: student modelling and adaptive learning systems.[170] The student modelling is important in the implementation of Learning Management Systems (LMS).[171] Thus, the student's profile is an important element of the LMS because it is used to centralise all the information that is associated with a particular student (e.g. his/her name, educational background, career progression etc.). With student profiling, the LMS gives the opportunity to educators to provide online courses for students, to test their achievements and manage their educational process.

Profiling is also important for adaptive (or personalised) systems such as intelligent tutoring systems. By applying profiling techniques, for example, a university may predict the probability of a student to graduating or not and thus be able to provide support for that student. Adaptive systems are very promising for the educational community. Their vision is to create an advanced and effective educational environment where each student will have his/her own personal tutor, thereby addressing many problems regarding the progress of each student.[172]

vi. Social Media, Social Networks and the Web

Social media and social networks are perhaps the most important areas of profiling practices today. The growth and use of social media and networks have generated unprecedented amounts of social data. Social networks (e.g. Facebook, LinkedIn, Instagram, Twitter) provide easily an accessible platform for users to communicate and interact with each other and share information on a daily basis. Users make transfers, conduct business, and socialise with friends on the Internet. With all of this information available (for free), online data has become a unique source for online profiling. The opportunities that arise from the mining of such data are of great potential for organisations of all kinds.

[170] Hildebrandt and Backhouse 2005, FIDIS Deliverable D7.2 (n 8) 61.
[171] 'LMS are electronic learning environments providing support to the online management, delivery and tracking of learning'.
[172] Ferraris, Bosco and D'Angelo 2013b (n 162) 11.

Another interesting aspect in the field of online profiling is the mining and monitoring of website users' data. These data can be processed to produce knowledge to 'target advertisements, personalise web sites and match services to a specific customer's needs'.[173] For example, controllers apply behavioural profiling (or online behavioural targeting) to track users and build profiles based on their characteristics, interests, lifestyle and shopping activities.[174] Therefore, a business entity can use profiling techniques to address customers' preferences and recommend to them goods and services that reflect their interests according to their profiles.

As the above analysis reveals, the use of profiling practices provides business entities with a powerful instrument to discover valuable knowledge about individuals and their lives. Basically, profiling enables the disclosure of unknown or forgotten information regarding individuals' pasts or presents, their identities, behaviour, locations, health or even their mental and emotional state of mind.[175] This capability of business entities may lead to the abuse of the rights of the data subjects and may directly or indirectly affect their lives. Thus, the following chapter will explore the various implications of profiling in an attempt to determine how and to what extent the use of profiling may threaten the fundamental rights and values of individuals and, consequently, their rights to privacy and the protection of personal data.

[173] Patrick 2000 (n 128) 56.
[174] Ferraris et al. 2013a (n 79) 29.
[175] Gary T. Marx, 'Privacy and Technology' (1990) The World and I <http://www.worldandi.com/> (accessed 10 July 2015).

Chapter 2

Profiling and Its Challenges

> *'The more I use the service, the more information it will have and the better it will get. It will know me better than I know myself. And at the same time, because it is making decisions for me, it will also influence (…) the person I am to become. (…) Now if the Web sites continually suggest new things for me to read and I accept their suggestions, it will influence my intellectual development (…). The more I accept their choices, the more likely I am to like the next choice (…). Over time, one could say that rather than the computer profile reflecting my tastes, I reflect its tastes'*[176]

2.1. Introduction

The use of profiling technologies has enabled the distribution of information and knowledge at an unprecedented level. Today, individuals live an electronic life through their computers and/or mobile phones. They make transfers, conduct business and socialise with friends in the digital world of the Internet. In the course of these activities, individuals may disclose their names, addresses, credit card numbers, social security numbers, their marital, educational or financial status, as well as health problems, political or religious beliefs, habits, sexual preferences and love affairs.[177] Consequently, this 'technology-rich lifestyle'[178] has dramatically increased the volume of information generated by each individual and enables the observation and monitoring of the individual's behaviour and activities through the use of profiling technologies.

At the same time, this information has become an asset and valuable tool for many business entities. The continuous collection, processing and analysis of this information, by profiling technologies, allows the automatic identification and

[176] Richard T. Ford, 'Save the Robots: Cyber Profiling and Your So-Called Life' (2000) Stanford Law Review 52(5) 1573–1584.
[177] Vera Bergeson, 'It's Personal but Is It Mine? Towards Property Rights in Personal Information' (2003) University of California, Davis Law Review 37(2) 379; Adam L. Penenberg, 'The End of Privacy' (1999) <http://www.forbes.com/forbes/1999/1129/6413182a.html> (accessed 19 November 2015).
[178] Francesca Bignami, 'Privacy and Law Enforcement in the European Union: The Data Retention Directive' (2007) Chicago Journal of International Law 8(1) 235.

categorisation of individuals into certain profiles based on their behaviour and preferences and helps business entities to make decisions in order to build their business models, improve their services and increase their profits. For instance, information collected from customers about product returns (e.g. whether the product was as expected, size fit, if the customer changed his/her mind etc.) enables the business entity to discover possible problems with the returned products or any changes in customers' preferences. The aggregation of such data helps the business entity to offer new, higher-quality products that reflect the customers' preferences and standards.[179] In addition, these data may also be combined with other data that the customer left behind while surfing other websites with similar or different products, and this gives to the business entity additional information about the life, preferences and needs of the customer. In this way, profiling technologies enable business entities to adjust their services based on the personal interests of each customer.

However, by monitoring all individuals' activities, profiling technologies enable different types of information to be merged to link to individuals' offline lives and thus to their physical identities. The use of facial recognition technology, otherwise known as face-to-data (F2D), for instance, can infer different types of information about a person based on the image of that person's face.[180] This F2D, if combined with different images posted on social media sites, can link to names and other information about the people in the images. Consider the following scenario: a man takes a photo of a woman in the street. If that photo is combined with that woman's publicly available Facebook profile, it can give the woman's name, home address and telephone number and, through this information, may infer additional (and even sensitive) information about her (e.g. marital status, educational level, habits, job etc.).[181]

It follows, therefore, that profiling technologies allow for the collection and processing of information and the monitoring of individuals' behaviour and activities

[179] Mary Culnan, '"How Did They Get My Name?" An Exploratory Investigation of Consumer Attitudes Towards Secondary Information Use' (1993) MIS Quarterly 17(3) 341.
[180] Christopher Kuner and others, 'Face-to-data---another developing privacy threat?' (2013) International Data Privacy Law 3(1) 1.
[181] Kuner et al. 2013 (n 180) 1.

that are meant to be private. This means that profiles constitute the digital representation of the real world of individuals.[182] As a result, the use of profiles may have a direct impact on the lives and fundamental values of individuals and thus give rise to privacy and data protection issues.

The purpose of this chapter is to examine the possible challenges that arise from the use of profiling in order to determine how and to what extent individuals are affected by the creation of profiles and the decisions made based on those profiles. This formulation helps to understand how concerns about the protection of fundamental rights and values of individuals are related to profiling and how profiling can occupy such deep and serious legal emotions, and thus why profiling is privacy-invasive.

This chapter is structured as follows: in section 2.2 the chapter focuses on the question of 'what is profiling all about?'. It explains the substance of profiling through the creation of a new type of knowledge based on individuals' past, current and future characteristics and activities. Section 2.3 aims to explore the potential challenges posed, by the use of profiling, to the fundamental rights and values of individuals in order to determine how and to what extent individuals are affected by the creation of profiles and the decisions made based on those profiles. Based on those challenges, section 2.4 explains how the classification of individuals in profiles may create potentials for a segmented society with considerable effects on the basic fundamental rights and freedoms of individuals, and shows how profiling may challenge democracy and the structure and welfare of society. In doing this, the section discusses Michel Foucault's ideas about the Panopticon and explains how profiling may create conditions of social control, social sorting and normalisation of individuals. Finally, section 2.5 deals with the challenges of profiling to democracy.

[182] Arnold Roosendaal, *Digital Personae and Profiles in Law: Protecting Individuals' Rights in Online Contexts* (Wolf Legal Publishers 2013) 99.

2.2. What is Profiling all about?

As explained in the first chapter of this thesis, profiling can be understood as the automatic processing and analysis of data for the creation of profiles in order to uncover hidden patterns and correlations within the databases. These profiles allow business entities to discover unknown and potentially useful knowledge about their customers based on the patterns of their previous behaviour. Basically, profiling enables the disclosure of information which is unknown or forgotten regarding individuals' past or present preferences, characteristics and behaviour.[183] As Mireille Hildebrandt argues, profiling makes the invisible visible.[184] Thus, even though individuals may not want to disclose certain information about themselves to others, profiling makes possible the prediction of this information.

However, profiling does not only provide information about individuals' past and current characteristics and behaviour but also it discovers new knowledge as to the future condition, behaviour and activities of the individual who is being profiled.[185] In other words, profiling makes feasible the prediction of individuals' futures. Such predictions can be based on data that have been collected from different sources and include information about the individual or the group profiles to which the individual belongs.[186] The paradox of these future predictions is that they may constitute unknown information for the individuals themselves. Individuals do not know what will happen to them in the future or how they will act or decide in a future situation (e.g. if they will not be able to pay their loan in ten months' time, if they will need a new car in a year or if they will buy a flat instead of a house etc.).

To illustrate this, consider the example of a student loan business entity which is collecting information about its student loan holders. By using profiling, the business entity can know, for instance, when these students graduate, where they live, when

[183] Marx 1990 (n 175).
[184] Mireille Hildebrandt, 'Who is Profiling Who? Invisible Visibility' in Serge Gutwirth et al. (eds), *Reinventing Data Protection?* (Springer 2009) 241.
[185] Hildebrandt 2009b, (n 184) 241.
[186] Bart Custers, 'Predicting Data that People Refuse to Disclose: How Data Mining Predictions Challenge Informational Self-Determination' (2012) Privacy Observatory Magazine < http://www.privacyobservatory.org/> (accessed 12 November 2015).

they pay off their loans, what kind of job they are looking for or if they pay their bills on time. This information can be used to discover whether these students are likely to purchase a car or a house in the future or whether they will be good scoring clients for opening a bank account, obtaining a credit card or being accepted for a future loan.[187]

As a result, all this new information ascribes new characteristics to individuals and enables business entities to customise their services accordingly. In this way, business entities can make decisions on behalf of individuals which might affect their lives and their future opportunities (e.g. if a student is evaluated as a future good scoring client he/she may be characterised as a 'good' client and as a result he/she may be offered better loan rates whereas other students who are not evaluated as future good scoring clients may be excluded from such opportunities).

Two crucial questions arise in relation to the knowledge about individuals' futures: Do individuals need or want to know about their future? If they do know their future, how this will affect their lives and future choices? In relation to the first question, there is not a 'Yes' or 'No' answer. There are individuals who may want to know about their future and others who may not want to know. Of course, every individual would want and, in any case, should be entitled to be aware that a business entity knows and keeps information about his/her future and to have the right to object to the maintenance, processing and dissemination of such knowledge. In relation to the second question, obtaining knowledge of his/her future may be beneficial or harmful for the individual, as the case may be. For example, knowledge of a potential future health problem will give an individual the opportunity to act preventively by making better choices to avoid it. However, this will mean that individuals will organise their lives according to what they know about their future. This will limit their options and govern their present and future behaviour. As a result, the person will not live according to his/her own dreams, goals and values but on the fear of a probable future situation. Nonetheless, all the data which are related to the future conditions of the individual, irrespective of the type and the nature of the data, must be legally

[187] Stevens L, 'IT Sharpens Data Mining's Focus – Instead of Building Data-Mining Application with No Clear Goal. Companies are Setting Priorities Up Front to Maximize ROY' (6 August 2001) Internet Week 29.

considered as sensitive data,[188] so that the same data cannot be stored, processed or used without the knowledge and approval of the individual.

So viewed, the following section will examine how and to what extent the disclosure of past, current and future knowledge about individuals' characteristics and activities, as well as the decisions made based on this knowledge (profiles), are likely to affect individuals' rights and lives.

2.3. Challenges to Individuals

The current section identifies and analyses the challenges posed to individuals by the use of profiling technologies in order to understand how privacy and data protection concerns are related to profiling. These challenges concern surveillance, asymmetries of knowledge, manipulation and threats to autonomy, discrimination, de-individualisation, stigmatisation, stereotyping and inaccuracy in the information and decision-making process.

2.3.1. Surveillance

Profiling facilitates continuous and real-time surveillance of individuals through their data.[189] As is mentioned in the first chapter of this thesis, Roger Clarke defined profiling as a data surveillance or dataveillance technique which involves the 'systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons'.[190] Thus, using profiling technologies, business entities can trace and track individuals' online and offline behaviour and activities. Location devices, for example, like GPS (Global Positioning Satellite) can locate and monitor individuals not only in fixed places, but also trace and track people while they are *on the move* using their smart phones,

[188] Please see Article 9 GDPR and section 4.7 in Ch 4 for further explanation on sensitive data.
[189] Surge Gutwirth and Mireille Hildebrandt, 'Some Caveats on Profiling' in Serge Gutwirth et al (eds), *Data Protection in a Profiled World* (Springer 2010) 31.
[190] See text to n 19 in Ch 1.

doing their shopping, visiting a bank, driving or walking in the street.[191] As a result, the data collected through this tracking (e.g. location data, voice data, image data, biometric data etc.) can lead to constant observation of individuals in most aspects of their lives whether online or offline, at home, at work, on the road and so on.[192]

A key aspect of data surveillance is that it strengthens business entities' capacities for both collecting and combining data from multiple sources as well as organising and transforming such data into valuable knowledge. By continuously tracking individuals' activities, a business entity can discover information about individuals' activities and behaviour and then combine this information with other data, collected by third parties, in order to create customers' profiles. All smart phones, for example, can reveal individuals' locations by the signals the phones are sending to the nearest antenna.

Therefore, by allowing immediate uploading of geo-tagged photos, videos and messages to different sites (e.g. YouTube, Facebook, Twitter), or by encouraging users to frequently 'check in' their positions, business entities can disclose not only information about a user's location but also information related to their habits and everyday life (e.g. a person frequently 'checking in' at a gym infers that this person likes sports and healthy living).[193] Based on these findings, the business entities can follow every movement of their customers and adjust their services accordingly. The Yowza!! Application, for example, provides its users with a service that automatically locates discount coupons for stores and restaurants in the user's current geographical location. In other words, business entities are making decisions that concern or affect their customers based on the constant observation of their actions.

[191] David Lyon, 'Introduction' in D. Lyon (ed), *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination* (Routledge Publishing 2003) 5.
[192] Gutwirth and Hildebrandt 2010 (n 189) 34.
[193] Gerald Friedland and Robin Sommer, 'Cybercasing the Joint: On the Privacy Implications of Geo-Tagging' (2010) International Computer Science Institute <http://www.icsi.berkeley.edu/pubs/techreports/TR-10-005.pdf> (accessed 5 October 2015).

2.3.2. Knowledge Asymmetries

One of the problems of profiling is that it creates knowledge asymmetries that result in the unbalanced distribution of powers between data subjects and the controllers.[194] Profiling technologies allow business entities to collect and analyse a vast amount of individuals' data in order to create profiles that will give them new knowledge about their current or potential customers. In most cases, however, individuals are not aware of the consequences of the use of those profiles on their lives, on their identities and on their future choices. They are not aware of the amount of data about themselves that are available to the public (through the Internet) and the extent to which these data may link to their offline lives and to their physical identities. Neither do they know the purposes for which a profile may be used and by whom. As Serge Gutwirth and Mireille Hildebrandt stated:

> 'Citizens whose data are being mined do not have the means to anticipate what the algorithms will come up with and hence they do not have a clue what knowledge about them exists, how they are categorized and evaluated and what effects and consequences this entails'.[195]

Consequently, this lack of awareness results in a lack of control over their data. This is because once the data have been circulated to the Internet, they are no longer under the individual's control.[196] As a result, the lack of control creates asymmetries of knowledge between controllers (who obtain new knowledge about individuals from the created profiles) and individual subjects (who are not aware of the profiles applied to them). Knowledge asymmetry may affect the level of power between business entities and customers.[197] The effect of this imbalance of powers may lead to unfair treatments for the customers (e.g. different prices for different types of customers) and unfair manipulation of a person's future choices or actions (e.g.

[194] Bosco et al. 2015a (n 13) 10.
[195] Gutwirth and Hildebrandt 2010 (n 189) 5.
[196] Hildebrandt and Backhouse 2005, FIDIS Deliverable D7.2 (n 8) 12.
[197] Schermer 2011 (n 100) 47.

customers are forced to buy products that they are not initially interested in).[198] Inevitably, therefore, knowledge asymmetries and imbalance of powers generate questions about the protection of the basic fundamental rights and values of the individuals.

2.3.3. Manipulation and Threats to Individual Autonomy

In the sphere of privacy, knowledge asymmetries and imbalance of powers pose threats to the autonomy of the individual and the freedom to self-develop his/her personality and identity in order to effectively participate within society.[199] The value of autonomy entails the capacity of individuals to make their own choices and live according to their own wishes and goals. This means that individuals should be free to express themselves without any fear of being judged by others because of their behaviour and choices.

From a privacy perspective, individual autonomy refers to the right of a person to self-determination and freedom to exercise his/her rights in a democratic society. Self-determination entails the capacity of a person to control his/her life and to live freely according to his/her own wishes. John Fischer explains that 'the value of a life is a narrative value and free will is valuable insofar as it allows us to shape the narrative structure of our lives'.[200] Thus, individuals are free if they can control the narrative structure of their lives.

In the context of information privacy (otherwise known as data protection), autonomy refers to informational self-determination. Informational self-determination means that individuals need to have control over their personal information.[201] In this sense, individuals are free to shape the narrative structure of their lives if they have control over their personal information and any decisions

[198] Bart W. Schermer, 'Risks of Profiling and the Limits of Data protection Law' in Bart Custers et al. (eds), *Discrimination and Privacy in the Information Society: Data Mining and Profiling in Large Databases* (Springer 2013) 139.
[199] Nancy J. King and Pernille Wegener Jessen, 'Profiling the Mobile Customer – Privacy When Behavioural Advertisers Target Mobile Phones – Part I' (2010) 26 Computer Law & Security Report 461.
[200] John Martin Fischer, 'Free Will, Death and Immorality: The Role of Narrative' (New York: Oxford University Press 2009) 152.
[201] Ferraris, Bosco and D'Angelo 2013b (n 162) 3.

made based on that information. Allowing individuals to exercise control over their personal information means that the individuals have the right to preserve their individual autonomy, integrity and dignity and thus to develop their own identities and personalities in order to participate freely in the social, economic and political life of society.[202] Therefore, individuals are free to shape the narrative structure of their lives if they preserve their autonomy and 'live an existence that may be said "self-determined"'.[203] This implies that individuals should be free from external interventions in order to make their own choices and their own decisions.

According to Fischer, individuals are not free to shape the narrative structure of their lives if either there is a lack of individuals' capacities to participate in the decision-making process or if the individuals are subject to manipulation by external entities.[204] In either case, although individuals' lives might still have narrative value, such value is not freely chosen by the individuals themselves but is attributed to them by others (the external entities).[205]

Profiling enables business entities to make decisions on behalf of individuals based on their past behaviour and actions without the individuals' knowledge. Based on these decisions, business entities can manipulate individuals' choices by influencing, for example, their willingness to participate in certain activities or their willingness to buy a certain product or service.[206] For instance, if a customer is unaware that a profile applies to him/her for marketing purposes, he/she may be forced to buy a product that he/she would not buy otherwise[207]. Such manipulative practices can be conducted by either limiting the types of the products they offer to a particular customer, by offering to him/her better prices for certain products, or by tailoring advertising banners based on his/her personal interests in order to force him/her to

[202] Antoinette Rouvroy and Yves Poullet, 'The Right to Informational Self-Determination and the Value of Self-Determination: Reassessing the Importance of Privacy for Democracy' in Serge Gutwirth and others (eds), *Reinventing Data Protection?* (Springer 2009) 45–76.
[203] Rouvroy and Poullet 2009 (n 202) 45–76.
[204] Fischer (ed) 2009 (n 200) 152.
[205] Fischer (ed) 2009 (n 200) 152.
[206] Tal Z. Zarsky, 'Mine Your Own Business!': Making the Case for the Implications of the Data Mining of Personal Information in the Forum of Public Opinion' (2002–2003) Yale Journal of Law & Technology 5(1) 38–40.
[207] Zarsky 2002–2003 (n 206) 38–40.

buy a certain product.[208] A good example of this kind of practice is that provided by Tal Zarsky in one of his articles:

> 'Mr. Orange often purchases through an e-commerce grocer and has recently stopped buying cigarettes. The grocer, anxious to cash in on potential lucrative tobacco sales, notices that Mr. Orange has just purchased a "nicotine patch" and concludes that he is trying to quit smoking. Mr. Orange is then presented with cigarette ads at the websites he visits, and even receives a "complimentary" cigarette pack in his most recent grocery shipment'.[209]

In Zarsky's example, the grocery store is interfering with Mr. Orange's autonomy and his capacity to make decisions about his life. The knowledge discovered by the profiling process (i.e. that Mr. Orange is trying to quit smoking) and the purpose for which the profile is used (i.e. to prevent Mr. Orange from quitting smoking) allow the grocery store to influence Mr. Orange's choice to quit smoking by targeting him with cigarette advertisements and by offering him a 'complimentary' cigarette pack. Mr. Orange is neither aware of being profiled nor that the grocery store is trying to prevent him from quitting smoking. As a result, Mr. Orange might decide to receive that 'complimentary' cigarette pack on his next purchase without realising that he has been influenced and that decision is not actually his own autonomous decision but the grocery store's decision.

Evidently, the use of profiling interferes with individuals' autonomy and self-determination. Without the awareness of being profiled, individuals cannot preserve their autonomy and exercise their right to self-determination. The lack of knowledge revealed by the profiling process, and the purposes for which the profile is intended to be used, may reduce individuals' capacities to control their lives and make their own autonomous decisions. In addition, by limiting individuals' options in order to force them to buy a certain product, it also reduces their ability to freely make choices and control their lives. In speaking about free will, Roman Altshuler argued

[208] Zarsky 2002–2003 (n 206) 20.
[209] Zarsky 2002–2003 (n 206) 20.

that free will presupposes that individuals should have 'the ability to choose between alternative possibilities'.[210]

Moreover, profiling allows business entities to customise their services according to each individual's needs. These needs are inferred from the past behaviour and choices of the individuals and thus any decisions made based on these needs are in fact based on individuals' pasts (e.g. past tastes, past habits, past purchases, past visits, etc.). For example, Amazon suggests to its customers books they might like to read based on their previous reading choices (e.g. the type of the book, the language written or the author).

In this way, profiling forces people to live based on their past and prevents them from making new choices. According to Fischer, individuals should be able to learn from their past choices, to move on and make better and/or different choices.[211] For him, the narrative structure of life allows individuals to change or improve their lives, not only 'by adding more good to them, but by changing the value of past misfortunes and by making something good come of them (…)"'.[212] In other words, individuals should be able to change their past behaviour and choices and not be captivated by them because a good choice today does not necessarily imply that it will be a good choice for tomorrow.

Profiling, therefore, is likely to reduce individuals' capacities to freely shape the narrative structure of their lives and make their own autonomous decisions, by creating people with limited knowledge and by manipulating their wishes and directing their choices in order to enforce them to act or decide in a certain way (in favour of their manipulators). Thus, a question arises about whether manipulation of this kind amounts to duress. The answer to this question is not easy or simple because a lot of factors, and the particular circumstances of each case, must be taken into consideration.

---

[210] Roman Altshuler, 'Free Will, Narrative, and Retroactive Self-Constitution' (2014) *Phenomenology and the Cognitive Sciences* (ISSN: 1568-7759 (print) 1572-8676 (online)) 1
[211] Fischer (ed) 2009 (n 200) 152.
[212] Fischer (ed) 2009 (n 200) 152.

According to Steyn LJ in case *CTN Cash and Carry Ltd. v Gallaher Ltd*: '(…) the fact that the defendants have used lawful means does not by itself remove the case from the scope of the doctrine of economic duress (…)'.[213] Additionally, in Chitty on Contracts it is stated as follows:

> '[t]here is no doubt that difficulty and delicate problems may arise in deciding whether threats otherwise lawful can amount to duress in the particular circumstances of the case. It seems that the court would have to take account of a wide range of factors in making such a decision, including (for instance) the nature of the threat; whether such a threat is commonly regarded as a legitimate way of exerting pressure; how coercive the threat is in the particular circumstances in which the party threatened is placed; what alternative remedies he may have, and how effective such remedies would be; the nature of the demand coupled with the threat; the nature of the consequences to the threatened party if he submits to the coercion on the one hand, and if he refuses to submit on the other; and the identity and status of the parties (…)'.[214]

Bearing in mind the meaning of duress, as above, and that the burden to prove it is on the customer, it is doubtful whether the customer can prove that manipulation amounts to duress. Nevertheless, under certain circumstances the customer can prove that manipulation amounts to 'undue influence', which '(…) is a comprehensive phrase covering cases of undue influence in particular relations and also cases of coercion, domination or pressure outside those special relations (…)'.[215]

---

[213] *CTN Cash and Carry Ltd. v Gallaher Ltd* [1993] EWCA Civ 19.

[214] Chitty on Contracts 25th edition, para 489, p. 276 (UK: Sweet & Maxwell Ltd 1983); See also Chitty on Contracts 30th edition, para 7-003 (UK: Sweet & Maxwell Ltd 2008).

[215] Chitty on Contracts 27th edition, para 7-024 (UK: Sweet & Maxwell Ltd 1994); See also *Universe Tankships v International Transport Workers Federation*, The Universal Sentinel [1983] 1 AC p 400.

2.3.4. Discrimination

Arguably, profiling practices are associated with the issue of discrimination. The word discrimination derives from the Latin word *discriminate* which means to 'distinguish between'.[216] Discrimination refers to biased treatment towards individuals on the basis of their membership of different groups or categories, rather than on individual merit (e.g. a person is treated according to his/her membership of a certain religion or ethnic minority group).[217] In other words, discrimination means 'denying to members of one group opportunities that are available to other groups'.[218]

The ability of controllers to collect, combine and analyse data from various sources enables the classification and categorisation of individuals into profiles based on certain characteristics. These characteristics are used to make automated decisions about individuals like accepting them for a job, granting them a loan or selling them a certain product. As a result, the application of profiles is likely to facilitate unfair treatments towards individuals and may create discrimination against certain categories or groups of individuals. For instance, business entities may provide limitations on certain services for specific groups of individuals (e.g. high income customers are excluded from receiving discount coupons).[219]

In a legal context, the right to non-discrimination constitutes one of the fundamental principles of European law.[220] It comprises the right to equality which requires that

---

[216] Salvatore Ruggieri, Dino Pedreschi and Franco Turini, 'Data Mining for Discrimination Discovery' (2010) ACM Transactions on Knowledge Discovery from Data Journal 4(2) 1.
[217] Indre Žliobaitė, Faisal Kamiran and Toon Calders 'Handling Conditional Discrimination' (2011) ICDM '11: Proceedings of the 2011 IEEE 11th International Conference on Data Mining 992; See also Ruggieri 2010 (n 216) 1.
[218] Sara Hajian and Josep Domingo-Ferrer, 'A Methology for Direct and Indirect Discrimination Prevention in Data Mining' (2013) IEEE Transactions on Knowledge and Data Engineering 25(7) 1445.
[219] Simone van der Hof and Corien Prins, 'Personalization and Its Influence on Identities, Behaviour and Social Values' in Mireille Hildebrandt and Serge Gutwirth (eds), *Profiling the European Citizen: Cross-Disciplinary Perspectives* (Springer 2008) 121.
[220] Article 21 of the EU Charter states: '1. Any discrimination based on any ground such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation shall be prohibited. 2. Within the scope of application of the Treaty establishing the European Community and of the Treaty on European Union, and without prejudice to the special provisions of those Treaties, any discrimination on grounds of nationality shall be prohibited.' See also Article 14 of the European Convention of Human Rights and Article 14 of the UK Human Rights Act 2000.

people in equal cases should be treated in the same way and people in different cases should be treated differently (e.g. men and women should be treated equally in employment matters).[221] In this respect, on 1st March 2011, the Court of Justice of the European Union (ECJ), in examining the *Test-Achats case*,[222] which was referred by the Belgian Constitutional Court, declared invalid as from 21st December 2012 the exemption in the EU equal treatment legislation, provided by Article 5(2) of the Council Directive 2004/113/EC.[223] Article 5(2) allowed Member States to maintain differentiations between men and women and gave them a right to derogate from the unisex rule with regard to insurance contracts. Belgium made use of this derogation and included a derogation for life insurance in its national legislation. The Court found that the exception to the unisex rule in Article 5(2) was incompatible with the purpose of Directive 2004/113/EC and consequently with the EU's Charter of Fundamental Rights, and ruled that the derogation was invalid.[224]

Discrimination can be either direct or indirect. In order to prevent discrimination based on sex, Directive 2004/113/EC applies to both direct and indirect discrimination. Direct discrimination occurs when a person is treated less favourably than others in equal circumstances on the basis of sensitive characteristics such as religion, ethnicity, gender, criminal or medical records and sexual preference.[225] Indirect discrimination occurs when non-sensitive characteristics are strongly correlated with biased sensitive ones and generate discriminatory impact on individuals or groups.[226]

The distinction between direct and indirect discrimination is relevant in profiling because the data collected to classify individuals into profiles may directly or indirectly involve sensitive characteristics for the individuals. Thus, direct discrimination in profiling occurs when decisions are made based on sensitive

[221] Ferraris et al. 2013a (n 79) 9.
[222] *Association belge des Consommateurs Test-Achats ASBL and Others v Conseil des ministers* Case C-236/09.
[223] Directive 2004/113/EC of the Council of the European Union of 13 December 2004 implementing the principle of equal treatment between men and women in the access to and supply of goods and services OJ L 373, 21/12/2004 P. 37–43.
[224] *Test-Achats case*; See also Hato Schmeiser, Tina Störmer and Joël Wagner, 'Unisex Insurance Pricing: Consumers' Perception and Market Implications' (2016) In *The Geneva Papers*, Palgrave Macmillan, London.
[225] Directive 2000/43/EC of the Council of the European Union of 29 June 2000 implementing the principle of equal treatment between persons irrespective of racial or ethnic origin OJ L 180, 19/07/2000 P. 0022–0026.
[226] Directive 2000/43/EC; See also Hajian and Domingo-Ferrer 2013 (n 218) 1445.

characteristics (e.g. a person may be excluded from receiving a car loan because of his/her gender or age) while indirect discrimination occurs when decisions are made based on non-sensitive characteristics which are strongly correlated with biased sensitive ones (e.g. a woman with children may be rejected from a job interview because the business entity believes that mothers will need more time off from work in order to take care of their children).[227]

In profiling, discrimination may occur either at the data collection stage or at the data analysis stage. At the collection stage, if the collection of historical data by a certain device (e.g. a CCTV camera in a bank) is organised manually by human experts to focus on a certain minority group (e.g. foreign customers), the CCTV camera will tend to focus on the individuals within this group even when the individuals are not showing signs of suspicious behaviour. As a result, the historical data will include more events involving foreign customers than non-foreign customers since they are the people who are being constantly observed. Consequently, the historical data will contain discrimination towards foreign customers and the analysis of these data will produce discriminatory results that will lead to discriminatory decisions in the future (e.g. foreign customers are excluded from loan or mortgage granting).[228]

Discrimination at the data analysis stage may occur when the 'predictive data mining algorithms may "learn" to discriminate on the basis of biased data used to train the algorithm'.[229] If the training data are biased against certain groups or classes of individuals, the learned model will also show discriminatory results about those groups or classes of individuals. Such discriminatory results are likely to allow future discrimination. In other words, if the training data are biased against foreign customers, the system might infer that every foreigner should be excluded from loan or mortgage granting.

Discrimination may also occur when profiling reveals knowledge as to the sensitive characteristics of an individual. This is the case of indirect discrimination. In this

[227] Bosco et al. 2015a (n 13) 14.
[228] Zarsky 2002–2003 (n 206) 28.
[229] Schermer 2013 (n 198) 139.

case, if the training data are biased against those sensitive characteristics they are likely to learn the discriminatory relationship with these characteristics and thus to give discriminatory results when applied to new data in the future.[230] For example, if a business entity systematically refuses to hire gay people as its employees, the historical data of this business entity concerning job applications will be biased in favour of offering jobs to heterosexual people while denying applications from homosexual people. It is important to note, however, that the mere fact of removing the sensitive characteristics from the training data does not necessarily preclude indirect discrimination if the non-sensitive characteristics in the training data are closely related to the sensitive ones.[231] If, for example, race is related to the remaining non-sensitive characteristics such as home address or income level, the learned model will still show discriminatory results towards individuals of a certain race. A typical example of indirect discrimination is 'redlining' practices through which business entities refuse to offer certain products or offer low quality products to certain geographical areas because of the ethnic origin of their population.[232] Wells Fargo, for instance, an American multinational banking and financial services business entity which is also engaged in services for lending houses, was sued for suggesting to its customers houses according to their current zip code. The result of such suggestions was that customers living in particular neighbourhoods with specific ethnic backgrounds and low incomes were referred to houses in specific areas only.[233]

2.3.4.1. Personalised Pricing and Advertising Schemes

The most common discriminatory practices in profiling are the creation of personalised pricing schemes (discriminatory pricing) and advertising promotions (discriminatory advertising). Discriminatory pricing is the business entity's ability to

[230] Kamiran and Žliobaitė 2013 (n 217) 156.
[231] Kamiran and Žliobaitė 2013 (n 217) 156.
[232] David Phillips and Michael Curry, 'Privacy and the Phenetic Urge: Geodemographics and the Changing Spatiality of Local Practice' in David Lyon (eds), *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination* (Routledge Publishing 2003); See also Hajian and Domingo-Ferrer 2013 (n 218) 1445.
[233] Mike Hatch, 'The Privatization of Big Brother: Protecting Sensitive Personal Information from Commercial Interests in the 21st Century' (2001) 27 William Mitchell Law Review 27(3) 1457; Dee De Pass, 'Wells Fargo Pulls Criticized Data; Housing Information on Company's Web site is Labelled Racist (BUSINESS)' Star Tribune (Minneapolis, MN) (23 June 2000) <https://www.highbeam.com/doc/1G1-63044933.html> (accessed 13 December 2015).

provide the same products and services at different prices to different customers according to each customer's past transactions and purchase behaviour. In this way, as Zarsky stated, business entities can 'create [a] different "store" for every customer by providing them with a different screen or window'.[234] In other words, every customer is treated separately and differently (one-on-one marketing) according to his/her profile.[235] For example, business entities, based on their customers' profiles, can provide to each customer a mail order catalogue with the same products but with different prices.[236]

By using profiling, the business entity can predict the price each customer is willing to pay for a product or a service and, as a result, manipulate prices according to each customer's requirements.[237] For example, if the collected data show that a customer is unconcerned about the price of the product, unaware of competing prices or in a hurry (e.g. the customer is always buying from the same online grocery store during his/her lunch breaks), then the system might infer that the customer shows a high willingness to pay for a product and he/she might be overcharged.[238] However, the customer is not aware of the fact that the price he/she pays when purchasing the product will affect the price he/she will be charged in the future.[239] As a result, a customer who has showed a high willingness to pay for a product will be recognised as a customer willing to pay high prices and he/she will repeatedly receive high prices.[240]

There are three degrees of price discrimination.[241] First degree price discrimination is based on individuals' preferences. This means that the business entity offers the same services to different customers based on their willingness to pay for that service. In second degree price discrimination the individual chooses among

[234] Tal Z. Zarsky, 'Desperately Seeking Solutions: Using Implementation-Based Solutions for the Troubles of Information Privacy in the Age of Data Mining and the Internet Society' (2004) Maine Law Review 56(1) 52.
[235] Zarsky 2002–2003 (n 206) 30.
[236] Roberta Brody, 'Consequences of Electronic Profiling' (1999) IEEE Technology and Society Magazine (Spring) 20.
[237] Alessandro Acquisti, 'Identity Management and Price Discrimination' (2008) IEEE Security and Society (March/April) 47.
[238] Zarsky 2004 (n 206) 53.
[239] Zarsky 2002–2003 (n 206) 26.
[240] Alessandro Acquisti and Hal R. Varian, 'Conditioning Prices on Purchase History' (2002) SIMS <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=336684> (accessed 23 October 2015).
[241] Acquisti and Varian 2002 (n 240); See also Acquisti 2008 (n 237) 47.

different prices for different versions of services. In other words, the business entity provides various options (e.g. high quality or standard quality) with equivalent prices. In third degree price discrimination the prices are targeted to different customer segments based on certain attributes. The degree of price discrimination that a business entity will choose to adopt for each customer depends on the type and volume of information that is known for each customer.[242]

Customer behaviour and status affects the pricing policies of the business entities and leads to pricing discrimination. For example, the customer who travels in business class, buys expensive clothes and eats in expensive restaurants will be charged higher prices that the customer who travels in economy class, buys normal clothes and eats in cheap restaurants. Also, a young person behaves differently towards a product and its price than an older customer.[243] Specifically, depending on age, geographical location, education, employment status, financial status, social class, lifestyle and shopping habits, and also on the combination of these factors, the business entities choose the price they adopt for each customer and each customer behaves responsively to the price so adopted.

In the case of discriminatory advertising, business entities can use profiling to customise their marketing strategies. They adjust their advertisement banners according to the results of each customer's profile (e.g. food, books or clothes preference). Thus, the banners are offering different products and services, adjusting prices and creating different types of offers and discounts based on each customer's prior purchase behaviour.[244] In this way, business entities are recommending different products and services to different customers. For instance, many online supermarkets send their frequent shoppers messages to inform them when their favourite products are back in stock or they offer them discount coupons or low prices in order to reward them, while other customers do not receive such offers (e.g.

[242] Acquisti and Varian 2002 (n 240); See also Acquisti 2008 (n 237) 47.
[243] Bee-Lia Chua et al., 'Impacts of cruise service quality and price on vacationers' cruise experience: Moderating role of price sensitivity' (2015) *International Journal of Hospitality Management* 44 131–145.
[244] Zarsky 2002–2003 (n 206) 22–31.

frequent customers receive 20% discount for birthday cakes on their birthdays).[245]

As a consequence of the above described discriminatory practices, business entities are encouraged to focus on more profitable customers and to give less attention to individuals with less income. The use of CRM (Customer Relationship Management)[246] profiles in the banking sector, for example, enables a bank to identify the bank's most profitable customers by analysing a variety of factors (e.g. a customer's salary, marital status, education, debts, property owned etc.) and as a result to devote more time and attention to them than to less profitable customers.[247] According to Seamus McMahon (former executive vice president of First Manhattan Consulting Group (1995–1999) and now president at McMahon Advisory in New York), the application of CRM profiles can create conditions in which unprofitable customers may be charged higher account fees or they may receive lower service than profitable customers because the bank does not want them (e.g. an email from a profitable customer will be answered more quickly than an email from an unprofitable customer).[248]

Clearly, the example of CRM profiles indicates that profiles constitute a source of discrimination for business entities. They facilitate the adoption of different treatments for different types of customers by either offering different services to certain groups of individuals or by excluding certain individuals from their services.[249] At the same time, the division of the market between profitable and non-profitable customers can create groupings and stereotypes within society. These conditions can cause social and ethical harm to individuals and create concerns over their fundamental rights and values and, in particular, over the rights to privacy and

[245] Acquisti and Varian 2002 (n 240) 6.
[246] CRM is defined as 'a combination of business process and technology that seeks to understand a company's customers from the perspective of who they are, what they do, and what they are like' (see Couldwell C, *A Data Day Battle, Computing* (1998) 64).
[247] Semih Onut, Ibrahim Erdem and Bora Hosver, 'Customer Relationship Management in Banking Sector and A Model Design for Banking Performance Enhancement' in Ali Minai and Yanner Bar-Yam (eds), *Unifying Themes in Complex Systems IV: Proceedings of the Fourth International Conference on Complex Systems* (Springer 2008) 370.
[248] Lynda Edwards, 'Big Banker is Watching: In the Brave New Banking World, "Unprofitable" Customers Will Find that Bankers don't Want them – or their Money' (22 January 1999) Bankrate.com <http://www.bankrate.com/brm/news/bank/19990122.asp> (accessed 9 November 2015).
[249] Zarsky 2002–2003 (n 206) 22.

the protection of personal data.[250]

2.3.5. De-individualisation

One of the problematic aspects of profiling is that the creation and application of profiles may affect the individuality of the person.[251] Profiling creates models of behaviour through the process of generalisation and categorisation of individuals into groups. Group profiling offers more opportunities for business entities to select their potential targets. Nonetheless, the use of group profiling generates a number of concerns. The search for patterns and correlations within the data may lead to serious effects for group members because of the risk to the members of being identified on the basis of the group characteristics and not on their own individual characteristics.[252]

In this way, an individual is judged and treated as a member of a particular group rather than an individual as such.[253] For example, a person 'X' may be refused a loan on the basis that he belongs to a certain group profile (e.g. living in a particular neighbourhood in which people have a higher chance of not paying their loans), whereas the person 'X' himself is a very reliable person who pays his bills on time and has a good income. Therefore, a group characteristic may be used in a way that is prejudicial to a member of the group. This is because a wrongful presumption of a person's individual characteristics or identity may result in that person's de-individualisation or stigmatisation within society.

De-individualisation is 'the loss of a person's sense of individuality and personal responsibility'.[254] Instead of acting as an individual, a person who is experiencing

[250] Zarsky 2002–2003 (n 206) 22.
[251] Anton Vedder, 'KDD: The Challenges to Individualism' (1999) Ethics and Information Technology 278.
[252] Bart Custers, 'Effects of Unreliable Group Profiling by Means of Data Mining' in Gunter Grieser, Yuzuru Tanaka and Akihiro Yamamoto (eds), *Discovery Science*: *6th International Conference, DS 2003, Sapporo, Japan, October 17-19, 2003. Proceedings* (Springer 2003) 291; See also Scherme 2013 (n 198) 47.
[253] Kristen Wahlstrom et al., 'On the Ethical and Legal Implications of Data Mining' (2006) Technical Report SIE-06-001 (School of Informatics and Engineering, Flinders University Adelaide, Australia); See also Vedder 1999 (n 251) 277.
[254] The Free Dictionary, <http://www.thefreedictionary.com/deindividuation> (accessed 25 April 2015).

de-individuation becomes 'lost in a group'.[255] This means that a person will follow the group and do whatever the group is doing (e.g. a teenage student may feel a sense of unity with the other students in his class and start behaving in the same way as his classmates). Thus, the person becomes less individual and more anonymous.[256]

In profiling, de-individualisation is more likely to happen in the case of non-distributive profiles where the characteristics of a group profile do not necessarily mean that they constitute the characteristics of the individual as such. These characteristics only represent the individual as a member of the group. For instance, a person may be refused a life insurance policy on the basis of his/her membership in a group profile which shows a high probability risk of being involved in a car accident (e.g. 'fast car drivers') whereas if this person is considered individually (as such) he will be excepted from such a risk because that person is a very careful driver and his 'fast car' is a vintage 1968 Porsche 912 which he drives only during the weekends.

The consequences of the use of non-distributive profiles may differ according to whether the characteristic of the group is evaluated as negative or positive.[257] A person who is mistakenly evaluated with a negative characteristic (e.g. group of high-risk people with certain health problems) can be excluded from a service (e.g. his/her life insurance application is rejected) while a person who is mistakenly evaluated with a positive characteristic (e.g. group of healthy people) may be included in a service (e.g. his/her life insurance application is accepted) that he/she may not be qualified to receive. In either case, the person is evaluated and treated unfairly and inaccurately.

According to Ed Diener, a person is de-individuated if he/she develops the following characteristics: firstly, a person shows lack of self-awareness (the person adopts the behaviour of the group and loses his/her individual emotions, thoughts and actions);

---

[255] Laura Freberg (Professor of Psychology at California Polytechnic State University), 'What is De-individualisation? <http://psych.answers.com/social-psychology/what-is-deindividuation> (accessed 25 April 2015).
[256] Katelyn Y. A. McKenna and John A. Bergh, 'Plan 9 from Cyberspace: The Implications of the Internet for Personality and Social Psychology' (2000) Personality and Social Psychology Review 4(1) 61.
[257] Wahlstrom et al. 2006 (n 253).

secondly, a person does not see him or herself as a separate entity but as a part of the group (the person shows less attention to him or herself); thirdly, a person lacks self-regulation (the person has lost control over him or herself).[258] Following these characteristics, de-individualisation can result in the loss of an individual's identity and self-differentiation (i.e. 'individual's sense of being a separate entity in a social environment'[259]). This is because a de-individuated person is more vulnerable to external conditions and is therefore more likely to adopt the group's characteristics.[260] Healthy people, for example, who are mistakenly evaluated as unhealthy (because of their membership of a group of unhealthy people) and repeatedly receive advertisements for junk food, may start being vulnerable to these advertisements and end up eating junk food. As a result, these people may lose their healthy lifestyle and adopt the unhealthy eating habits of the group profile in which they were classified.

It follows, therefore, that classification of people in profiles may change their preferences and behaviour by forcing them to develop the habits and tastes of the group. Thus, people are not the same as before their classification in the profile.[261] Ian Hacking points out that those classifications affect the people classified and the effects on the people, in turn, change the classifications:

> 'We think of these kinds of people as definite classes defined by definite properties. As we get to know more about these properties, we will be able to control, help, change, or emulate them better. But it's not quite like that. They are moving targets because our investigations interact with them, and change them. And since they are changed, they are not quite the same kind of people as before. The target has moved. I call this the "looping effect". Sometimes, our sciences create kinds of people that in a certain sense did not exist before. I call this "making up

[258] Ed Diener, 'Deindividuation: The Absence of Self-Awareness and Self-Regulation in Group Members' in P. Paulus (ed), *The Psychology of Group Influence* (Lawrence Erlbaum 1980) 209–242.
[259] Arie Nadler, Marta Goldberg and Yoram Jaffe, 'Effects of Self-differentiation and Anonymity in Group on Deindividuation' (1982) Journal of Personality and Social Psychology 42 1127–1136.
[260] Nadler, Goldberg and Jaffe 1982 (n 259) 1127–1136.
[261] Ian Hacking, 'Making Up People' (2006) London Review of Books 28 (16) 23–26.

people"'.[262]

This 'making up' of people depends on the context of the profiles and the decisions made for their application (how, to whom and for what purposes a profile will be applied). What is important is that such 'making up' encourages loss of control and separation from the real self. Profiling, therefore, does not only categorise individuals according to their past behaviour and characteristics but it may also create new behaviours and new identities. As such, profiling can create serious social effects on individuals' lives because 'individuals may be given an identity that is not of their choice'.[263]

2.3.6. Stigmatisation

Profiling may also lead to the stigmatisation of an individual or a group if the knowledge discovered in the profile becomes publicly available.[264] For example, there is a general perception that online dating sites are only for people who cannot find a date. Therefore, people who visit such sites often do not want others to know due to the fear that other people may stigmatise them as desperate.

A stigma can be defined 'as a sign or a mark that designates the bearer as defective and, therefore, as meriting less valued treatment than "normal" people'.[265] Therefore, stigmatised individuals are those 'who by virtue of their membership in a social category are vulnerable to being labeled as deviant, are targets of prejudice or victims of discrimination, or have negative economic or interpersonal outcomes'[266] (e.g. black people have fewer economic opportunities and lower incomes and thus are less successful than white people). In other words, stigmatised individuals are marked with certain characteristics which create for them a social identity that is not

[262] Hacking 2006 (n 261) 23–26.
[263] Lee A. Bygrave, 'Data Protection Law: Approaching Its Rationale, Logic and Limits' (2002) 10 Information Law Series 291.
[264] Custers 2003 (n 252) 293.
[265] Monika Bieruat and John F Boridio, 'Stigma and Stereotypes' in Todd F. Heatherton et al. (eds), *The Social Psychology of Stigma* (The Guilford Press 2003) 88.
[266] Jennifer Crockers and Brenda Major, 'Social Stigma and Self-Esteem: The Self-Protective Properties of Stigma' (1989) Psychological Review 96(4) 609.

fully accepted by society.[267]

As a result, individuals in profiles with stigmatised characteristics may be denied respect and be socially rejected and excluded by other individuals. For example, many resource departments arrange job candidates in group profiles based on their qualifications and behaviour in order to evaluate their suitability for a job (e.g. 'poor' candidates' profiles, 'middling' candidates' profiles or 'hire away' candidates' profiles). If a person is being profiled as a 'poor' candidate and this information becomes publicly available, then this person can be stigmatised as unemployable and as a result may be rejected from future job opportunities even if he/she is mistakenly classified in the 'poor candidates' profile (e.g. because of his/her membership in a certain group on Facebook).[268]

According to the sociologist Erving Goffman, there are different types of stigmatisation. The most important types are those related to '"tribal identities" (e.g., race, sex, religion, or nation)', '"blemishes of individual character" (e.g., mental disorders, addictions, unemployment)' and '"abominations of the body" (e.g., physical deformities)'.[269] In the case of profiling, if a person or a group is identified as having a stigma based on the above categories, this will influence the way individuals' behaviour is understood and classified. Thus, information about a person having a certain degree of probability to develop a certain disease or behaviour because of his/her DNA results or lifestyle (e.g. unstable mental behaviour) is likely to give rise to stigmatisation and discrimination (e.g. denying insurance services, jobs or loans).

A good example for our discussion is the creation of profiles for the prediction of child abuse in New Zealand. The Ministry of Social Development in New Zealand is considering the use of profiling in order to stop instances of child abuse before they happen. By using government data provided by citizens (in exchange for social

[267] Jennifer Crocker, Brenda Major and Claude Steele, 'Social Stigma' in Daniel Todd Gilbert, Susan T. Fiske and Gardner Lindzey, *The Handbook of Social Psychology* (4th edn, Oxford University Press 1998) 505.
[268] Frank Pasquale, 'Op-Ed: We're Being Stigmatized by 'big data' Scores We don't Even Know About' (15 January 2015) Los Angeles Times <http://www.latimes.com/opinion/op-ed/la-oe-0116-pasquale-reputation-repair-digital-history-20150116-story.htm> (accessed 8 September 2015).
[269] Bieruat and Boridio 2003 (n 265) 88.

services), the Ministry intends to predict how likely parents are to abuse their children. The use of such profiles may lead to stigmatisation of parents as not good parents because there is a possibility that some parents may mistakenly be classified as 'high risk' parents (of harming their children) and thus be marginalised by society.[270] In addition, a person being profiled as a 'high risk' parent may also deal with more serious effects such as separation from his/her children.

Social rejection of stigmatised individuals can create lower expectations for acceptance from others and, therefore, prevent them growing and developing within society.[271] It may also create individuals with low self-esteem. Individuals tend to see themselves based on what other people believe or feel about them.[272] Shelley Duvas and Robert Wicklund argued 'that people are prone to self-evaluations based on broader social standards and norms'.[273] Accordingly, individuals being profiled as members of a stigmatised group may start to develop negative feelings and evaluate themselves according to the results of that profile. For instance, the parents that are evaluated as 'high risk' parents are likely to start seeing themselves as not-good parents while the candidates who are evaluated as 'poor' candidates are likely to start seeing themselves as not-good employees. Arguably, therefore, stigmatisation can lead to psychological as well as social consequences for the group members.[274]

2.3.7. Stereotypes

Another problem of profiling is the creation of stereotypes within society. Profiling is about generalisation of certain characteristics of a particular group or class of people. Stereotyping is also about generalisation. Generalisation is vital for the social

[270] Teresa Cowie, 'Beneficiaries Fear Profiling Stigma' (19 June 2015) <http://www.radionz.co.nz/national/programmes/insight/audio/201758628/insight-for-21-june-2015-child-abuse-or-big-brother> (accessed 8 September 2015).
[271] Deborah E. Reidy, '"Stigma in Social Death": Mental Health Consumer/Survivors Talk About Stigma in their Lives' (Education for Community Initiatives Holyoke, MA 1993) <http://akmhcweb.org/articles/StigmaisSocialDeath.htm> (accessed 8 September 2015).
[272] Amy L. Gonzales and Jeffrey T. Hancock, 'Mirror, Mirror on my Facebook Wall: Effects of Exposure to Facebook on Self-Esteem' (2011) Cyberpsychology, Behaviour, and Social Networking 14(1-2) 79.
[273] Shelley Duval and Robert Wicklund, 'A Theory of Objective Self-Awareness' (New York: Academic Press 1972).
[274] Bieruat and Boridio 2003 (n 265) 88.

and private lives of individuals.[275] Individuals tend to generalise people (e.g. men and women, rich and poor, black and white etc.) and objects (e.g. pens and pencils, flats and houses etc.) in order to understand the world and make their lives easier.[276] In doing so, they create categories – stereotypes – of people and objects within society.

A stereotype is referred to as 'the content of an assumed set of characteristics associated with a particular social group or type of person'.[277] Thus, stereotypes entail society's general impressions of a particular group or person. For example, lawyers are successful and earn high incomes, women are careless drivers, fat people eat too much, people who use online dating sites are desperate and so on. Like de-individualisation and stigmatisation, individuals who are stereotyped are treated according to the category they fit in rather than on their own individual conditions and merits. For instance, business entities create profiles consisting of people who share the same characteristics (e.g. 'high income customers', 'young professionals', 'vegetarian customers' etc.) and then adapt their marketing strategies and services according to each group's characteristics. In this way, business entities are treating all group members the same. Thus, group profiles do not reflect the personality of each individual member, but rather they become stereotypes because all group members are judged and treated in terms of the (stereotype) profile.[278]

Even though stereotypes are useful in the sense of helping people to simplify their lives, they can create negative effects for individuals. The lack of knowledge as to the differences between the members of a group can create wrongful impressions as to the real characteristics of a person and thus damage his/her identity. Additionally, as with stigmatisation, individuals in stereotyped profiles may also experience social rejection, exclusion and discrimination in their environment which can limit their potentials to develop. Therefore, stereotyping can also create people with low self-esteem.[279] Moreover, 'stereotypes are involved in stigmatisation to the extent that

[275] David Lyon, 'Surveillance as Social Sorting: Computer Codes and Mobile Bodies' in David Lyon (ed), *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination* (Routledge Publishing 2003) 21.
[276] Bieruat and Boridio 2003 (n 265) 88.
[277] Bieruat and Boridio 2003 (n 265) 89.
[278] Schermer 2013 (n 198) 139.
[279] Reidy 1993 (n 271); See also Gonzales and Hancock 2011 (n 272) 80.

(…) a specific set of characteristics is assumed to exist among people sharing the same stigma'.[280]

2.3.8. Quality and Inaccuracy in the Data and Decision Process

Another problem associated with profiling is the inaccuracy of the profiles. As it has already been explained in Chapter 1 of this thesis, profiling is a probabilistic knowledge in the sense that it involves a degree of variation and a chance of multiple possible outcomes.[281] A profile represents the likelihood of an individual's future behaviour and not his/her actual future behaviour. The 'success' of the KDD (Knowledge Discovery in Databases) process depends to a large extent on the quality of the collected data.[282] If the data collected from the past behaviour of an individual are inaccurate or incomplete, the patterns discovered from the mining of the data will also be inaccurate and any decision made based on that profile (patterns) will give wrongful or unfair results that can affect the application of the profile and the identity of the individual subject.

Inaccuracies in the collected data could be based on four factors: firstly, the controller has failed to notice some information in the collected data (in relation to an individual's behaviour) or has wrongfully interpreted the collected data (e.g. wrongful interpretation of an individual's behaviour); secondly, there is lack of uniformity between online and offline data (e.g. an individual's online and offline behaviour is not consistent); thirdly, the data collected are out of date; and fourthly, the data provided by the individual are untruthful or misleading.[283] All these factors can result in unreliable profiles and inaccurate decisions as to the purpose of their application.

Such inaccurate results can occur in both categories, descriptive and predictive data modelling, especially when the creation of a profile is based on other individuals'

[280] Bieruat and Boridio 2003 (n 265) 89.
[281] See Section 1.6.2 in Ch 1.
[282] Schermer 2013 (n 198) 48.
[283] Szde Yu, 'Behavioural Evidence Analysis on Facebook: A Test of Cyber-Profiling' (2013) Defendology Journal 16(33) 27.

data.[284] In the case of personal profiles, for instance, if the profile is created with data which are thought to belong to a specific individual whereas in fact such data belong to another individual (parts of the data or all of the data belong to another individual), the profile will be inaccurate as well as any decisions made based on this profile.[285]

This is because the knowledge produced by this profile will give wrongful information as to the personality and identity of the individual and thus any decision made on this knowledge (profile) will be inaccurate because, in reality, this profile is someone else's profile. This is clarified by the following scenario: Mr Jack Reed, a man with a low income and a mortgage loan, is receiving offers for very expensive products due to the fact that Mr Reed's personal profile categorises him as a high-value customer because of the fact that he is buying very expensive ties and drives a Ferrari. However, the information on Mr Reed's profile is inaccurate because it is not Mr Jack Reed who is buying expensive ties and drives a Ferrari, but Mr Reed Black, his neighbour.

Furthermore, the number of 'false positive' and 'false negative' results is also important for the accuracy of the decision-making process. Profiling produces new knowledge without establishing reasons for this knowledge. The KDD process is based on the 'right and wrong' approach.[286] This means that the algorithms used for mining the data do not question the results (whether right or wrong) according to each individual case but take the results as given ('Yes' or 'No').[287] In credit scoring practices, for example, if a customer is categorised as a high-risk customer based on his/her credit score and the bank rejects his/her application for new account, the applicant could not know the exact reason for his/her rejection because the system only provides a 'Yes' (application accepted) or a 'No' (application rejected)

[284] Hildebrandt, Gutwirth and Paul de Heart, 'D7.4: Implications of Profiling Practices in Democracy' (FIDIS 05 September 2005) FIDIS consortium <http://www.fidis.net/> (accessed 15 July 2015).
[285] Hildebrandt, Gutwirth and Heart 2005, FIDIS Deliverable D7.4 (n 284).
[286] Roosendaal (eds.) 2013 (n 182) 143.
[287] Hildebrandt and Backhouse 2005, FIDIS Deliverable D7.2 (n 8).

answer.[288]

A false positive result means that individuals who do not fit the profile are in fact fitted in the profile, whereas a false negative result means that individuals who do fit the profile are left out.[289] For example, Mary is categorised as a high-value customer of an online accessories store and she receives offers and suggestions for very expensive jewellery and bags due to the fact that Mary regularly visits online stores which sell expensive women's clothes and accessories and she travels very often to Paris and Milano. Although the information in Mary's profile is correct, the conclusion and application of her profile is not accurate because all these activities are part of her job as an assistant fashion editor at a well-known fashion magazine and her trips to Paris and Milano (payable by the magazine) are part of her duties when she accompanies her boss during fashion weeks. Therefore, Mary is falsely fitted in a profile that characterises her as a high-value customer whereas in fact she should not be fitted in this profile (false positive result).

The existence of false positives or false negatives could have serious effects for individuals. Classifying individuals in the wrong profiles and assigning to them incorrect 'worth' or 'risk' values means that individuals find themselves with new characteristics and identities that can limit their options and affect their decisions and choices.[290] Therefore, a false positive or a false negative value could result in false inclusions or false exclusions from different services such as opening a bank account, receiving a credit card, receiving a low premium for insurance coverage or being hired for a job.[291]

2.4. Challenges to Society

Having discussed the challenges posed by profiling technologies to individuals and to their fundamental rights to privacy and data protection, the next section will

[288] Hildebrandt and Backhouse 2005, FIDIS Deliverable D7.2 (n 8).
[289] Schermer 2013 (n 198) 140; See also Zarsky 2002–2003 (n 206) 47.
[290] Lyon 2003 (n 275) 21.
[291] Hildebrandt, Gutwirth and Heart 2005, FIDIS Deliverable D7.4 (n 284) 56; See also Zarsky 2002–2003 (n 206) 48.

examine the possible challenges that profiling may pose to society and democracy.

2.4.1. Profiling: A Segmented Society

One of the most important issues surrounding profiling concerns the segmentation of the market into different social and economic categories.[292] Profiling enables business entities to classify individuals into different categories and assign to them certain values (e.g. 'highly profitable customer', 'inaccurate employee' or 'high-risk mortgage payer') in order to determine who should be included or excluded from their services.

To achieve this, business entities are creating market segments that enable them to identify and target potentially profitable customers based on their geographic, psychographic or demographic characteristics.[293] David Phillips and Michael Curry speak about the 'phenetic urge': the classification of individuals based on their geodemographic similarities.[294] They explain how, today, the idea of 'you are where you live'[295] applies to classify individuals not only according to their geographic area but also according to their homogeneous lifestyles, behaviour and preferences.[296]

By dividing the market into different segments, business entities are classifying the population into groups.[297] In fact, business entities are creating different social and economic categories within society. In placing, therefore, customers in profiles based on their demographics, location, behaviour and lifestyle, profiling is dividing the population into new social and economic categories. The result of these divisions is the segmentation of society into 'poor or rich', 'healthy or unhealthy', 'mentally stable or unstable', 'educated or non-educated' and so on. Such resulting classification can change the structure and welfare of a society and create potentials

[292] Hildebrandt 2009b (n 184) 244.
[293] David M. Funsten, 'Helping your Customers Behave Themselves' (1998) Bank Marketing 30(10) 223–24.
[294] Phillips and Curry 2003 (n 232) 137.
[295] The idea of 'you are where you live' dates back to the nineteenth century and was developed in order to separate less well-off people from the community based on their geographic area of living. Thus, people living in small neighbourhoods were seen as having less financial value and were left behind with fewer opportunities (Phillips and Curry 2003 (n 232) 143).
[296] Phillips and Curry 2003 (n 232) 137.
[297] Lyon (ed) 2003 (n 275) 2.

for constant surveillance, social control, normalisation, discrimination and social sorting of the population.[298]

A good example to illustrate this is the Apple's 'News' Application. 'News' provides to iPhone and iPad users a personalised news service based on the topics and stories related to their personal interests. 'News' collects information from the links, pages, stories and topics that the user wants to read based on pre-selected topics of interest (e.g. business, sports, politics, fashion etc.) that the user has stored in his/her device. In this way, 'News' classifies its users into different profiles according to their topics of interests (e.g. 'business' readers, 'sports' readers, 'law' readers, 'technology' readers etc.) and provides to them news based on those profiles. This form of classification and information filtering can result in exclusions or inclusions of the users from certain sources and topics and thus limit or enhance their knowledge in relation to certain content or information (e.g. by providing to them specific types of information while disregarding others). As a result, business entities providing such services can take control over the knowledge the users are receiving and influence their opinions and thoughts on certain beliefs and ideas. Cass Sunstein considers profiling in terms of personalised filtering and emphasises two problems as a result of this filtering:

> 'First, people should be exposed to materials that they would not have chosen in advance. *Unanticipated encounters*, involving topics and points of view that people have not sought out and perhaps find irritating, are central to democracy and even to freedom itself. Second, many or most citizens should have a range of *common experiences*. Without shared experiences, a heterogeneous society will have a more difficult time addressing social problems and understanding one another'[299]

Subsequently, the use of 'News' and other similar filtering services (e.g. 'BBC

[298] Hildebrandt 2009b (n 184) 244; See also Lyon (ed) 2003 (n 275) 5.
[299] Cass Sunstein, 'The Daily We: Is the Internet Really a Blessing for Democracy?' (2001) Boston Review <http://bostonreview.net/cass-sunstein-internet-democracy-daily-we> (accessed 10 January 2015).

News' Application, 'Google News & Weather' Application, etc.) may entail the risks of impersonality and customisation of individuals' characters that may affect their freedom to self-develop their own unique identities within a democratic society. Individuals might be offered information that is not of their own choice, but rather is the choice of their profilers. This implies that individuals will not be opened to new opinions and ideas but they will be directed to change their beliefs to meet the beliefs of their profilers.[300] Accordingly, these services can cause knowledge asymmetries and imbalanced distribution of powers within society which may challenge democracy and the fundamental rights and freedoms of individuals.

These asymmetries and the imbalanced distribution of powers reflect the idea of Michel Foucault about the Panopticon – a disciplinary society.[301] The Panopticon is an architectural model for prisons designed by Jeremy Bentham in the nineteenth century.[302] The model structured the cells in such a way that they were open to a central panoptic tower (pan=all, optic=seeing). The prisoners, however, could not see if there was an inspector in the tower. The idea was to make them believe that they were being watched at any time.[303] Bentham believed that the feeling of constant observation would act as a control mechanism to tempt prisoners to adapt their behaviour – obey the rules – in order to avoid punishments.[304] The Panopticon, therefore, regulated the correction and control of prisoners' behaviour.

Michel Foucault used the Panopticon as a metaphor for the social control of individuals by public and private actors within society.[305] For him, the model of the Panopticon is a system of control and correction of individuals' behaviour that should be applied in different contexts of life (e.g. schools, workplaces, hospitals etc.) in order to ensure discipline within society:

> ' (…). Whenever one is dealing with a multiplicity of individuals on whom

[300] Solove (ed) 2004 (n 11) 44; See also Zarsky 2002–2003 (n 206) 41.
[301] Hildebrandt 2008b (n 184) 306; See also Oscar Candy, 'The Panoptic Sort: Political Economy of Personal Information (Critical Studies in Communication and in Culture Industries (Westview Press: 1993).
[302] Jeremy Bentham, 'Panopticon; Or, The Inspection-House' (Dodo Press 2008).
[303] Bentham 2008 (n 302).
[304] Michel Foucault, 'Discipline and Punish: The Birth of the Prison' (New York: Vintage Books 1977) 195–228.
[305] Foucault (ed) 1977 (n 304) 195–228.

> a task or a particular form of behaviour must be imposed, the panoptic schema may be used'[306]

Thus, Panopticon is the acceptance of and compliance with the rules. Individuals held in a Panopticon are directed to adopt disciplined behaviour because of the fear of being observed at any time. Consider, for example, CCTV cameras on the streets. Some of them are operating and some of them are not. However, individuals do not know which cameras are operating. They assume that they are the targets at any given moment. Fearing, therefore, at all times the eyes of the *inspectors*, individuals stop driving fast and adopt more careful driving behaviour. In other words, individuals, through their fear, are directed to shape their behaviour in a certain way, based on the needs of their *inspectors* – '[t]he judges of normality'.[307]

Nevertheless, for Foucault, the Panopticon meant much more than control over observation. According to him, control over individuals' behaviour is not solely based on their fear of being watched at all times but is also based on a further, deeper knowledge and analysis of the individuals' lives.[308] In his discussion and analysis of the Panopticon he also refers to the measures taken in a French town during the seventeenth century in order to deal with plague. According to these measures, it was decided to close the town and to prohibit all citizens from leaving their houses.

The town was divided into distinct quarters, each governed by an intendant, and each street was under the inspection of a syndic. In this way, they inspected all the actions of the citizens in order to 'ensure the prompt obedience of the people and the most absolute authority of the magistrates'.[309] Following this 'lock-down' and intensive surveillance, citizens then experienced a further and deeper observation:

> 'Based on a system of a permanent registration (…). At the beginning

[306] Foucault (ed) 1977 (n 304) 205.
[307] 'The judges of normality are present everywhere. We are in the society of the teacher-judge, the doctor-judge, the educator-judge, the "social worker"-judge; it is on them that the universal reign of the normative is based; and each individual, wherever he may find himself, subjects to it his body, his gestures, his behaviour, his aptitudes, his achievements' (Foucault (ed) 1977 (n 304) 304).
[308] Foucault (ed) 1977 (n 304) 196.
[309] Foucault (ed) 1977 (n 304) 196.

> of the "lock up", the role of each of the inhabitants present in the town is laid down one by one; this document bears the "name, age, sex of everyone, notwithstanding his condition" (…). Everything that may be observed during the course of the visits – deaths, illness, complaints, irregularities – is noted down and transmitted to intendants and magistrates. (…) The relation of each individual to his disease and to his death passes through the representatives of power, the registration they make of it, the decisions they take on it'.[310]

Thus, the model of the panoptic plague town was a system of identification, individualisation, classification of citizens into different categories and decision-making based on those categories.[311] The control of the plague citizens was being exercised not only through the fear of constant observation but also through division, differentiation and training of the citizens.[312] Within this context, Foucault argues that the power of control derives from the knowledge the observers have obtained, not only from their observation but also from the recording and deeper analysis of their individual objects.[313] For him, therefore, the model of the Panopticon is a system of control, correction, social classification of individuals and decision-making processes that facilitate the continuous observation and analysis of individuals for the purpose of ensuring discipline within society.

According to Foucault's model of the Panopticon, profiling facilitates a 'system of permanent registration' under which individuals' behaviour and activities are observed, processed, stored and classified in order to be managed and controlled in favour of the needs and interests of their *inspectors*. The eyes of the *inspectors* are the eyes of the controllers – business entities – that seek to control their individual subjects – their customers – in order to ensure *compliance* with their marketing strategies and their financial interests. The power to control derives from the collection, processing, combination and analysis of data which enables the constant

[310] Foucault (ed) 1977 (n 304) 196.
[311] Clive Norris, 'From Personal to Digital: CCTV, the Panopticon, and the Technological Mediation of Suspicion and Social Control' in David Lyon (eds), *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination* (Routledge Publishing 2003) 250; See also Candy 1993 (n 301).
[312] Foucault (ed) 1977 (n 304) 198–200.
[313] Foucault (ed) 1977 (n 304) 198–200.

observation and automatic classification of individuals in profiles. These profiles enable business entities to identify their potential customers and to discover valuable knowledge about various aspects of their lives in order to make decisions for their purposes and their benefits.

It follows, therefore, that profiling is creating a situation of panoptic surveillance under which the resulting distribution of powers may lead to social control, social sorting and normalisation of the population. As such, profiling does not only create issues of privacy but also issues of social justice and individual morality.

2.5. Challenges and the Rights to Privacy and Data Protection

The challenges described above are closely related to the fundamental rights to privacy and data protection. Both rights are necessary instruments for a democratic society. Privacy underpins human dignity and other key values of human life and has become one of the most important human rights of the modern age. Privacy is transformed according to the technological developments, 'the circumstances, the people concerned and the values of the society'.[314] According to Rachel Finn, David Wright and Michael Friedewald, privacy can be categorised into seven types: privacy of the person, privacy of behaviour and action, privacy of personal communication, privacy of data and image, privacy of thoughts and feelings, privacy of location and space and privacy of association.[315] On the other hand, personal data refers to any kind of information that can be used to identify an individual, either directly (e.g. name, address, photograph etc.) or indirectly through a combination of different data sources (e.g. online activities). The right to data protection has a broader scope than privacy in the sense that it provides protection for other fundamental rights like the right to freedom of expression, the right to freedom of religion and conscience and the right to equality and non-discrimination.[316]

[314] Bosco et al. 2015a (n 13) 18.
[315] Rachel L. Finn, David Wright and Michael Friedewald, 'Seven Types of Privacy' in Serge Gutwirth et al. (eds), *European Data Protection: Coming of Age* (Springer Science+Business Media 2013) 3.
[316] Bosco et al. 2015a (n 13) 18.

So viewed, even if the application of profiling is, at first glance, a positive tool for business entities, it entails a number of concerns as to the fundamental rights and values of individuals. The *exposure* of personal data may harm the identity and reputation of a person in society and violate his/her privacy. Interestingly, therefore, profiling poses a threat to the most basic and fundamental principles of law and to the relationships between controllers and their individual subjects.

Based on the above challenges, the next chapter provides an overview of the EU data protection legal framework in order to better understand the role of data protection in profiling practices as well as the importance of privacy and data protection as it derives from the fundamental values that both rights aim to protect.

Chapter 3

Data Protection and Privacy: The EU Legal Framework

3.1. Introduction

Profiling practices constitute a threat to a number of fundamental rights of individuals such as the right to privacy, the right to the protection of personal data, the right to non-discrimination, the right to due process and the right to the equality of individuals within society.[317] Among those rights threatened by the use of profiling practices, the right to privacy and the right to the protection of personal data are perhaps the most seriously challenged. Therefore, the present thesis addresses the threats that arise from the application of profiling to these two fundamental rights.

On the one hand, business entities are using profiling to collect, analyse and identify individuals' preferences and behaviour for the purpose of more effective personalised services (e.g. finding goods or services based on the needs of existing customers). Such practices may affect fundamental values and result in the violation of the individuals' rights to privacy and data protection. On the other hand, individuals embrace the benefits of personalised services offered as a result of profiling and, in some cases, they are willing to disclose their personal information in exchange for economic or social benefits (e.g. better bank rates or shopping discounts). Nevertheless, the majority of individuals are skeptical about disclosing their personal information because of their concerns over the threats to their privacy and personal data.[318] A 1998 Harris Poll, for example, indicated that the majority of the respondents were concerned about the threats to their privacy online and the way

[317] Bosco et al. 2015a (n 13).
[318] Mary J Culnan and Pamela K Armstrong, 'Information Privacy Concerns, Procedures Fairness, and Impersonal Trust: An Empirical Investigation' (1999) 10(1) *Organization Science* 104.

their personal information was used, while over 78% of the respondents stated that they would use the Internet more if their privacy was guaranteed.[319]

Similarly, a 2000 survey for the U.S. Federal State Commission demonstrated that the majority of the respondents did not trust business entities to keep their personal data confidential and over 64% of them expressed the view that they did not trust even those websites with posted privacy policies.[320] According to Mary Culnan and Pamela Armstrong, individuals' privacy concerns are reflected in two ways. Individuals are concerned about the unauthorised access to their personal data as a result of security absence or lack of internal controls, and about the risk of secondary use (re-use) of their data for purposes other than those the data is collected for without their consent.[321] According to them, these types of concerns reflect individuals' concerns about their rights to privacy and data protection. It is important, therefore, to examine how the EU legal framework protects these rights in order to determine the risks and perils that the law intends to prevent.

In using profiling technologies to collect, process, store and/or disseminate information, every business entity (controller) must comply with data protection legislation. Before turning to the relevant provisions of data protection legislation for profiling, it is necessary to address the fundamental rights of privacy and data protection within the EU legal framework, in order to understand their relationship as well as their importance as it derives from the fundamental values that both rights aim to protect.

The aim of this chapter is to provide an overview of the data protection legal framework in order to understand the importance of privacy and data protection as it derives from the fundamental values that both rights aim to protect. The chapter first highlights the relationship between data protection and privacy and examines the

[319] Harris Poll 1998 on Privacy <http://www.businessweek.com/1998/11/b3569104.htm> (accessed 10 June 2016).
[320] Division of Financial Practices, Bureau of Consumer Protection, 'Privacy Online: Fair Information Practices in the Electronic Market Place. A Report to Congress' (2000) <https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000text.pdf> (accessed 10 June 2018).
[321] Culnan and Armstrong 1999 (n 318) 104.

similarities and differences between the two rights (section 3.2). Sections 3.3 and 3.4 examine privacy, as the legal tool of opacity, and data protection, as the legal tool of transparency, in the light of the three basic fundamental principles of a democratic constitutional state. Based on the analysis of these three principles, the chapter provides a distinction between privacy as the legitimate opacity of the individual and data protection as the transparency of the controller. The next section discusses data protection as a legal tool for preserving and promoting a free and democratic society (section 3.5). The section also discusses data protection within the concept of the right to informational self-determination. Then, the chapter provides an overview of the EU data protection and privacy legal framework (section 3.6). Moreover, privacy and data protection are discussed as distinct fundamental rights under the EU Charter of Fundamental Rights. Section 3.7 explicates the genesis of data protection legislation as it has emerged from technological developments.

3.2. Privacy and Data Protection: Interacting Together *but* Existing Independently

Data protection has always been linked with the privacy of a person in such an extended way that it is difficult to assess its value and purpose without considering privacy. This is because the processing and dissemination of personal data has left no room for the legal community to consider a different notion of protection. Consequently, under EU law, both rights are established as fundamental legal rights (though not absolute), distinct from one another but related. Therefore, the two rights seem to have 'a parent–child relationship'.[322] Like a child who is closely related to his/her parents but tries to find his/her own way in life and build his/her own personality, data protection (as a child) is trying to establish its independent presence within the legal society while at the same time is retaining the *family bond* with privacy (as its parent).[323] Obviously, like a parent and a child, data protection and privacy interact in various ways with one another but at the same time they exist independently.

[322] Maria Tzanou, 'Data Protection as a Fundamental Right Next to Privacy? 'Reconstructing' a Not So New Right' (2013) International Data Privacy Law 3(2) 88–99.
[323] Tzanou 2013 (n 322) 88–99.

Privacy constitutes a vital element of a democratic society. It is a concept of multidimensional character and with a diversity of meanings. Privacy is transformed according to the technological developments, the needs, and the values of society. As an independent legal value, privacy was first developed in the nineteenth century when Professors Samuel Warren and Louis Brandeis proclaimed the need for a common law right to privacy – 'the right to be let alone' from any unwanted intrusions.[324] This way, Samuel Warren and Louis Brandeis had drawn the line between the rights of individuals to exercise their freedom and the extent to which public actors can interfere with such rights. Following this development, privacy is considered to involve other fundamental values such as the value of human dignity, individual autonomy, individual freedom, integrity and the value of self-development which entails the right of a person to freely develop his/her identity and personality.

The relationship between privacy and technology is complex. Technological developments have created countless threats to privacy. The potentials for computer systems to gather and store vast amounts of data create new possibilities for intruders (controllers) to invade individuals' privacy while at the same time the damages from such invasions seem to be unpredictable and can have severe effects on the lives of individuals. Thereby, the right to privacy needed to be reconsidered within the informational (technological) context in order to prevent illegal, unauthorised and unethical use of private information by new technologies. Within this broad notion, information privacy (or privacy of personal data) is considered as the ability of an individual to exercise power over his/her data and to influence the processing of such data and of any decision to be made or any knowledge that is to be obtained based upon such data.[325]

From a European perspective, information privacy is the right of information control, of limited accessibility and of non-interference with an individual's personal information (all of these terms have been incorporated in the EU data protection

[324] Samuel Warren and Louis Brandeis, 'The Right to Privacy' (1890) Harvard Law Review 4 193–220.
[325] Andrej Savin (ed), '*EU Internet Law'* (Edward Elgar Publishing Ltd. 2013) 190–218.

legislation).[326] For this reason, information privacy is connected with the concept of self-determination. Self-determination refers to the capacity of a person to control his/her life and live freely according to his/her own choices and his/her personality. In the informational context, informational self-determination means that 'an individual needs to have control over the data and information produced on him/her'.[327] However, individuals are not the legal owners of their personal information. Information is not an object of either copyright or property rights. This is because information does not pre-exist prior to its distribution, dissemination or publicity but it is always under construction by someone (controller). In this sense, information, even though it belongs to a person, is not his/her property.[328]

In this broad notion, data protection does not prohibit processing of personal data but allows it as long as the processing is not unfair and unlawful (both the DPD as well as the new GDPR provide that processing should be made for fair, legitimate and specific purposes and with the data subject's consent). Data protection covers the unfair and unlawful collection, processing and/or communication of an individual's personal data as long as the individual is identified or identifiable (under the EU data protection legislation).[329] These kinds of unlawful acts may occur when the data are collected and stored by a controller without the approval of the data subject (infringement by the act of intrusion) and/or when the data are disclosed to an unauthorised person for an unauthorised purpose without the approval of the data subject (infringement by the act of disclosure).[330]

As a result, data protection and privacy are related yet not identical rights. They are both affected by serious interference by governmental and private actors and they are both about protection of the individual's rights. However, data protection falls within the aspect of privacy in terms of information control over personal data (although not

[326] Lee A. Bygrave, 'The Place of Privacy in Data Protection Law' (2001) UNSW Law Journal 24(1) 277–283.
[327] Ferraris, Bosco and D'Angelo 2013b (n 162) 17.
[328] Federico Ferretti, 'Competition, the Consumer Interest, and Data Protection' in Federico Ferretti (ed), *EU Competition Law, the Consumer Interest and Data Protection: The Exchange of Consumer Information in the Retail Financial Sector* (Springer 2014) 93–119.
[329] Article 2(a) of the DPD defines 'personal data' as any information relating to an identified or identifiable natural person. 'Identified or identifiable natural person' means that the personal data are the data of a natural and not legal person.
[330] Federico Ferretti, 'The Credit Scoring Pandemic and the European Vaccine: Making Sense of EU Data Protection Legislation' (2009) 1 Journal of Information Law & Technology.

all personal data are considered private[331]). However, as it will be seen later, the right to data protection 'is more than informational privacy itself'.[332] It has a broader scope than privacy in the sense that it provides protection for other, further fundamental rights apart from privacy like freedom of expression, freedom of religion and conscience and the right to equality and non-discrimination.[333]

Therefore, although both rights protect the rights of the individuals, they have different roles to play. On the one hand, privacy has a normative (prohibitive) nature to protect the legitimate interests of individuals while data protection has a pragmatic (non-prohibitive) nature to ensure the fair and lawful processing of personal data by controllers. From this perspective, Paul De Hert and Serge Gutwirth[334] developed the theory that privacy is the legitimate opacity of the individual and data protection is the transparency of the controller (the powerful). According to them, opacity and transparency are legal tools that enable a democratic constitutional state to organise the relations between citizens' rights and social and state interests.

Opacity tools are closely related to the recognition of human rights and the autonomy of the citizens in a democratic society, whereas transparency tools have their origins in the principles of the rule of law of a democratic constitutional system. Before attempting to locate opacity and transparency as legal tools, it is essential to provide a conceptual background on the fundamental basic principles which govern a democratic society. This will help to understand how the tools of opacity and transparency work within a democratic society and how privacy, as an opacity tool, and data protection, as a transparency tool, find their origins within the basic principles of a democratic constitutional state.[335]

[331] Case T-194/04 *Commission v. Bavarian Lager Co. Ltd* [2007] ECR II - 4532, paras 118–119.
[332] Tzanou 2013 (n 322) 90.
[333] Ferraris, Bosco and D'Angelo 2013b (n 162) 18.
[334] Paul De Hert and Serge Gutwirth, 'Privacy, Data Protection and Law Enforcement: Opacity of the Individual and Transparency of the Power' in Erik Claes, Antony Duff and Serge Gutwirth (eds), *Privacy and The Criminal Law* (Intersentia 2006) 61–104.
[335] In this study the terms 'Democratic Constitutional State' and 'Democratic Society' are used as synonymous.

3.3. The Principles of a Democratic Constitutional State

The aim of a democratic constitutional state is to preserve social order in which the freedom of individuals is the primary concern. Thus, a democratic constitutional system should guarantee simultaneously order and a high level of individual freedom.[336] Otherwise, unlimited independence and self-reliance may create imbalances between the state's power and the individuals' freedoms and thus lead to the dissolution of the whole system. From this perspective, individuals' freedoms must be adjusted according to the social needs and be balanced with the interests of the state. On the other hand, the exercise of the state's power should be controlled and limited. For this reason, three basic fundamental principles – namely, the recognition of fundamental rights and freedoms, the rule of law and democracy – were enacted to ensure good practice and fair balance of interests within a democratic constitutional state.[337] These three principles will be discussed briefly below.

3.3.1. Fundamental Rights and Freedoms

In a democratic society, fundamental rights[338] are the rights that have been deemed, by law, to receive the highest degree of protection. They are of great importance for every individual. Their recognition and incorporation in the constitution highlights the duty and liability of the state to respect and protect them for all citizens in any circumstances.[339] In other words, fundamental rights indicate the power of the individuals within society and the limits of the state to intervene with these rights. Although, at first, the purpose was to protect individuals against the public administration, fundamental rights also protect individuals against other individuals or private actors. In this way, human rights have *positive* ('free from interference by others') and *negative* ('free to participate in public life') freedoms.[340] For the

[336] Hildebrandt, Gutwirth and Heart 2005, FIDIS Deliverable D7.4 (n 284) 11.
[337] Hildebrandt, Gutwirth and Heart 2005, FIDIS Deliverable D7.4 (n 284) 11.
[338] In this study the terms 'Fundamental Rights' and 'Human Rights' are used as synonymous.
[339] Roosendaal (ed) 2013 (n 182) 79.
[340] Isaiah Berlin, 'Two Concepts of Liberty' (1958) in Isaiah Berlin, *Four Essays on Liberty* (Oxford University Press 1969).

understanding of privacy, it is important to highlight that human rights mean those values that respect human life and dignity. Human rights constitute the protection of individuals as independent human beings separate from the state (the majority). Thus, human rights are about the autonomy and self-determination of the citizens within a democratic society.[341]

3.3.2. The Rule of Law

Rule of law means that no individual (whether a government official or a private citizen) stands above the law. The rule of law protects fundamental social, political and economic rights of individuals by limiting the power of the state. Again, the purpose is to defend individuals from the threats of the excessive exercise of governmental power. The difference is that the state is subject to the law and it can only exercise its powers in a legitimate way (according to that law). This implies that all powers must derive from the constitution and can only be exercised in accordance with the restrictions set out in the constitution.[342]

This suggests that a democratic constitutional state must be accountable (responsible for its actions), controllable and transparent (citizens must be aware of what is happening in the state) for the good of its citizens. The rule of law also involves the principle of equal treatment. The laws must be general and apply to all citizens in the same way (all individuals are equal before the law, equally valuable, with equal opportunities and equal treatment and should not be discriminated against because of their origin, their beliefs or their gender).[343]

Likewise, to prevent abuses of powers and balance the different interests within the state, the rule of law established the principle of the 'Separation of Powers'. 'Separation of Powers' refers to the division of a democratic constitutional state into three institutions or branches of administration: the *legislature* (responsible for

[341] De Hert and Gutwirth 2006 (n 334) 61–104.
[342] Costas G. Mavrias, '*Constitutional Law*' (3rd edn, Athens: Sakkoula Publications 2004) 137–142) (In Greek: Κώστας Γ. Μαυριάς (Τρίτη Έκδοση), *'Συνταγματικό Δίκαιο'* (Εκδόσεις Αντ. Ν. Σάκκουλα 2004) 137–142).
[343] Howard Cincotta, 'Democracy in Brief' (2007) Washington: U.S. Department of State, Bureau of International Information Programs <http://photos.state.gov/libraries/korea/49271/dwoa_122709/Democracy-in-Brief_kor.pdf> (accessed 10 August 2015).

initiating, approving or amending the law), the *executive* (responsible for enforcing the law), and the *judiciary* (responsible for interpreting and applying the law).[344] All three institutions are constitutionally obliged to work together and no one can exercise more power than the other. This separation of powers, therefore, limits the possibility of excessive and/or abusive exercise of power by the government 'since the sanction of all three branches is required for the making, executing, and administering of laws'.[345]

3.3.3. Democracy

A democratic constitutional state is devoted to the values of tolerance (of different opinions and behaviours), cooperation (between its citizens) and compromise (in conflicting disputes) in order to promote democracy among its citizens.[346] Democracy derives from the Greek word *'demokratia'* that was formed from *'demos'* (the people) and *'kratos'* (the power or rule).[347] In principle, the citizens of a democratic state must serve as the 'ultimate guardians'[348] of their own rights and freedoms.

This means that the power of the state derives from the supremacy of its citizens and the only valid and acceptable exercise of such power must be based on the will, the authorisation or the vote of the majority of the citizens (rule of the majority).[349] In other words, the system of a democratic constitutional state is a self-administered system where citizens govern themselves and the administrative power is justified if it is being exercised in favor of the good of the public interest (e.g. representation and participation of citizens in governmental institutions and in political decision-making bodies). In this way, the state authorities are directly and indirectly controlled by the citizens. As former President of the United States Abraham Lincoln

[344] CCHR Institutions Series, Separation of Powers and the Rule of Law (June 2011) <http://www.a4id.org/sites/default/files/user/Institutions_Fact_Sheet_1_Separation_of_Power.pdf> (accessed 18 August 2015).
[345] CCHR Institutions Series 2011 (n 344).
[346] Mavrias (ed) 2004 (n 342) 137–142.
[347] George Babiniotis, '*Dictionary of the Greek Language*' (2nd edn, Athens: Center of Lexicology Publications 2002) 471–472 (In Greek: Γεώργιου Μπαμπινιώτη (Β' Έκδοση), 'Λεξικό της Νέας Ελληνικής Γλώσσας' (Εκδότης Κέντρο Λεξικολογίας 2002) 471–472).
[348] Cincotta 2007 (n 343).
[349] Mavrias (ed) 2004 (n 342) 137–142.

stated in his famous phrase, 'democracy is government of the people, by the people [and] for the people'.[350] Following this, democracy also implies the accountability and transparency of the state towards its citizens.

3.4. Opacity and Transparency Tools

Having considered the way a democratic constitutional state functions under the three fundamental principles examined above, the tools of opacity and transparency will then be explored in order to determine the similarities and/or differences between privacy and data protection as well as the logic and scope behind the adoption of both rights.

3.4.1. Privacy as an Opacity Tool

Privacy as an opacity tool is the legal protection of the fundamental right of individuals against interference with their private and family lives by governments and private actors. In other words, privacy ensures opacity (non-interference) in individuals' autonomy and self-determination.

Opacity is the legal protection of individuals, their rights and their freedoms against interference by governments and by private actors. In other words, opacity is the legal protection of the fundamental rights to individual autonomy and self-determination and thus the protection of individuals' freedom to develop their own identities, personalities and selves within a democratic constitutional state. As such, opacity tools are legal tools that guarantee non-interference in the autonomy and freedom of individuals. They limit the exercise of power (by governments and private actors) against individuals' personal affairs.[351] That way opacity tools are normative in nature in the sense that in some cases 'the (constitutional) legislator takes the place of the individual'[352] and decides on his/her behalf of the unlawfulness

[350] Richard A. Epstein, 'Direct Democracy: Government of the People, by the People, and for the People' (2011) Harvard Journal of Law and Public Policy 34 819–826.
[351] Serge Gutwirth, 'Biometrics Between Opacity and Transparency' (2007) Ann Ist Supper Sanita 43(1) 61.
[352] De Hert and Gutwirth 2006 (n 334) 61–104.

of the interference. More simply, an act may infringe the autonomy of a person despite him/her consenting to this act (e.g. Article 3 of the EU Charter provides protection for the integrity of the person and explicitly prohibits certain acts of interference with the person's body[353]).[354]

Although, as an opacity tool privacy is normative and prohibitive in nature, it does not provide an absolute prohibition for non-interference. As it will be seen below, the law provides exceptions if certain conditions are met (e.g. 'according with the law' or 'necessary for a democratic society'). Accordingly, privacy is not an absolute fundamental right. Individuals do not have absolute control over their privacy. They have the freedom to exercise their rights up to the point they do not infringe the rights and interests of other individuals or the state. In essence, privacy aims to balance the legitimate opacity of the individual with the rights and interests of other individual citizens (the opacity of other individuals) as well as the interests of the society at large.[355] From this perspective, privacy provides both positive and negative freedoms. While the former protects individuals' rights and freedoms from governments and private actors, the latter protects individuals' rights and freedoms when such rights clash with other individual rights or with the public interests.[356]

3.4.2. Data Protection as a Transparency Tool

In principle, data protection law is a transparency tool. Considerably, the tools of transparency are different from the tools of opacity. They do not prohibit interference by governmental and private actors against individual matters, but they control such interference. Transparency tools regulate the acceptable level of the exercise of power. In other words, they make interference against individuals' rights

[353] Article 3 of the EU Charter states: '(1) Everyone has the right to respect for his or her physical and mental integrity. (2) In the fields of medicine and biology, the following must be respected in particular: the free and informed consent of the person concerned, according to the procedures laid down by law, the prohibition of eugenic practices, in particular those aiming at the selection of persons, the prohibition on making the human body and its parts as such a source of financial gain, the prohibition of the reproductive cloning of human beings'.
[354] De Hert and Gutwirth 2006 (n 334) 61–104.
[355] Hildebrandt, Gutwirth and Hert 2005, FIDIS Deliverable D7.4 (n 284).
[356] Berlin 1958 (n 340).

and freedoms legitimate up to a certain level.[357] It is for this reason that data protection law does not prohibit processing of personal data but regulates it. Thus, personal data can be collected, processed, recorded and disseminated, provided that certain conditions are met by the controller (e.g. fairness principle, openness principle, accountability principle, individual participation principle, etc.).

In this way, transparency tools make the controllers (government and public actors) transparent and accountable by regulating and controlling their actions and decision-making process in order to make them more responsible for the goodness of individuals.[358] Basically, the law provides the right to process data while at the same time limits this right by requiring the processing to be fair and lawful for the individual. Compared with opacity tools, transparency tools have a pragmatic nature. The law infers that governments and private actors need to be able to process personal data for social and economic purposes and that these purposes outweigh the privacy interests of the individuals.[359]

3.4.3. Privacy (as Opacity) and Data Protection (as Transparency)

As it is evidenced from the above analysis, both tools have the same ultimate legal purpose which is to limit and control the use of power over individual matters, but they approach it differently. Opacity tools protect individuals by prohibiting unlawful and excessive use of power, while transparency tools do not prohibit but regulate the accepted use of power. Therefore, privacy (as opacity) and data protection (as transparency) are different in their scope and logic. Privacy has a more general target to regulate the reasonable and the unreasonable acts of interference. It is 'much more than accountability and foreseeability'.[360] Alternatively, data protection has a more specific target distinct from privacy: the fair and lawful processing of personal data. For example, consider that a person applies opacity and transparency tools to restrict people's entrance to his/her house. With opacity

[357] De Hert and Gutwirth 2006 (n 334) 61–104; See also Hildebrandt, Gutwirth and Hert 2005, FIDIS Deliverable D7.4 (n 284).
[358] De Hert and Gutwirth 2006 (n 334) 61–104; See also Hildebrandt, Gutwirth and Hert 2005, FIDIS Deliverable D7.4 (n 284).
[359] Gutwirth 2007 (n 351) 63.
[360] De Hert and Gutwirth 2006 (n 334) 61–104.

(privacy) he/she closes the door to any person who tries to visit the house and opens it only to certain people like friends and family or technicians – *reasonable visitors* – whereas with transparency (data protection) he/she leaves the door open for any person to enter or invade the house (allows processing) as long as the entrance or invasion fulfil certain standards (e.g. fair and lawful processing).

In addition, opacity and transparency 'presupposed each other'.[361] Even though the default position of privacy is opacity and the default position of data protection is transparency, both rights provide exceptions. This means that privacy can provide transparency rules when, for example, telephone tapping is allowed under strict conditions (e.g. by law, for certain incriminations, limited in time etc.) and data protection can also provide opacity (prohibitive) rules where, for example, sensitive data are at hand (e.g. data relating to racial or ethnic origin, religious or political beliefs, criminal or health records or sexual preference).[362]

3.5. Data Protection as a Legal Tool for Preserving and Promoting a Free and Democratic Society

There is no doubt, following the above analysis, that privacy and data protection alike have their origins in the notion of the three basic fundamental principles of a democratic constitutional state. Data protection, as well as privacy, is a legal and social tool for preserving and promoting a free and democratic society. Transparency is a fundamental attribute of a democratic society and a basic norm for the protection of human rights. It is a legal tool used to achieve effective relations and to promote political and economic prosperity. Without transparency and accountability a state is undemocratic.[363]

Therefore, data protection is not only intended to protect the rights of the data subjects (individuals) and the interests of the controllers (public and private entities) but also to encourage and ensure democracy. This implies that data protection is a

[361] Gutwirth 2007 (n 351) 63.
[362] Hildebrandt, Gutwirth and Hert 2005, FIDIS Deliverable D7.4 (n 284).
[363] Mark Fenster, 'The Opacity of Transparency' (2006) IOWA Law Review 91 885–949.

legal tool to protect the fundamental values of a modern (informational) democratic society where individual citizens are left free and independent (from any action of control, from any observation or monitoring of their behaviour, preferences and feelings, from any actual or predictive profiling, from any categorisation and discrimination and from any automatic decision-making on their behalf) to exercise their rights and freedoms. Enabling individuals to exercise control over their personal data means that individuals are given the right to preserve their individual autonomy, integrity and dignity and thus to develop their own identities and personalities in order to participate freely within the social, economic and political life of society.[364]

Of course, to what extent it is possible to guarantee protection of fundamental rights within a profiling-based society and whether a mere control, by way of consent, is enough to provide effective protection for these rights, is something that will be examined later in this thesis.

3.5.1. Data Protection and the Right to Informational Self-Determination

As already stated above, data protection as a transparency tool constitutes an essential element of democracy and of the protection of fundamental values within a society. Hereinbelow, a survey of the fundamental values protected within the concept of data protection will be introduced in order to understand the importance of data protection legislation and the way data protection responds to the protection of these values.

Data protection should not only be understood as a mechanism for the control and management of personal data but also as a protection that entails other fundamental rights and values (individual autonomy, human dignity and self-development). Undoubtedly, the most accurate interpretation of data protection legislation is that given by the German Constitutional Court in 1983, in its landmark 'census decision'

[364] Rouvroy and Poullet 2009 (n 202) 45–76.

(Volkszählungsurteil).[365] The German Court, having seen data protection within the sphere of self-determination, developed the right to informational self-determination ('informationelle Selbstbestimmung'). This new right, according to the German Court's ruling, has its basis in Article 1 (human dignity) and Article 2 (personality right) of the German Constitution (Basic Law of the Federal Republic of Germany).[366]

In this way, the German Court explicitly created a link between data protection and the fundamental values of human dignity and self-development.[367] The value of self-development incorporates the right of a person to freely develop his/her personality and identity and thus the right to preserve his/her individual autonomy as a member of a free and democratic society. Following the approach of the German Court, data protection legislation does not only provide rights for the personal interest of the individual to be exercised solely in his/her private territory (away from the public eye), but considering that data protection is an essential element of a free and democratic society, these rights are also provided for the interaction of the individual with other individuals or the state. From this perspective, the rights given to individuals under the data protection legislation are also 'participatory rights'.[368] Such rights allow the individual to develop his/her own unique personality and identity in order to participate freely (without any fear of judgement) in the social, economic and political life of society.

Further, there is another value that data protection law is intended to protect: the value of 'trust'.[369] In today's information age, where profiling and data mining techniques are increasingly using data to predict information about individuals and to make automatic or semi-automatic decisions on their behalf, trust is perhaps one of the most important values that data protection intends to secure for individuals. According to Giovanni Sartor, trust can be defined as 'one's expectation that another

[365] Volkszählungsurteil BVerfGE 1, 68–69 (1983).
[366] Article 1(1) states that: 'Human dignity shall be inviolable. To respect and protect it shall be the duty of all state authority'. Article 2(1) states that: 'Every person shall have the right to free development of his personality insofar as he does not violate the rights of others or offend against the constitutional order or the moral law'.
[367] Rouvroy and Poullet 2009 (n 202) 54.
[368] Ferretti 2014 (n 328) 93–119.
[369] Ferretti 2014 (n 328) 93–119.

will act in a way that is advantageous to oneself, supplemented by one's ability to act upon such expectation, accepting the corresponding risk'.[370] More simply, trust is the willingness of an individual (trustee) to be vulnerable to the actions of another individual (trustor) while acknowledging the existence of a risk towards the exercise of these actions. In an informational context, trust is the willingness of a data subject to be vulnerable to the actions of a controller irrespective of the ability of the latter to observe, record, process, and/or disseminate his/her information. This implies that the 'data subject–controller' relationship involves a level of risk that the data subject acknowledges.

Trust, therefore, is a necessary precondition for the creation of any relationship within society, whether for private, social, political or economic purposes. Without trust a person cannot coexist with other individuals and he/she cannot develop his/her personality. Trust is necessary because it ensures the willingness and the desire of an individual to be an active and effective part of society. This presupposes that a state and its citizens must be transparent and accountable in order for trust to exist. In this way, data protection provides rights which affect all aspects of the individual's life (whether as a mere citizen, as a consumer, as an employee, as a businessperson and so on).[371]

Exploring the values that data protection should protect, it is clear that data protection is not only about informational self-determination as such – mere control – but is a fundamental right that entails all fundamental values that privacy is related to and intended to protect. Thus, data protection legislation should acknowledge and respect those values and should be 'interpreted in the light of those values'.[372]

A high level of data protection, therefore, is crucial to enhance trust in online services and to fulfil the potential of the digital economy, in order to encourage economic growth and the competitiveness of industries. However, the application of profiling practices enables the interception of data or the observation and monitoring

[370] Giovanni Sartor, 'Privacy, Reputation, and Trust: Some Implications for Data protection' in Ketil Stolen et al. (eds), *Trust Management* (Springer 2006) 354–356.
[371] Ferretti 2014 (n 328) 93–119.
[372] Rouvroy and Poullet 2009 (n 202) 54.

of behaviour and activities that are meant to be private. These kinds of abuses invariably affect the fundamental rights and freedoms of individuals and may violate the person's rights to privacy and data protection.

3.6. The EU Legal Framework

Until the enactment of the Lisbon Treaty in 2009 (which explicitly established protection of both the right to privacy and the right to data protection), the legal protection for the processing of personal data was supported through the legal channels of privacy. In order to understand, therefore, the nature and importance of data protection rights, it is necessary to examine the formation and development of privacy as a fundamental legal right.

This section provides a historical background of the right to privacy and the evolution of data protection rights within the EU as a result of new technological developments.

3.6.1. Privacy: 'From Open Windows to Closed Doors'

Privacy underpins human dignity and other key values of human life and has become one of the most important human rights of the modern age.[373] As already mentioned, privacy is being transformed according to the technological developments, the needs and the values of society.[374] It is perhaps the only human right that has been universally difficult to define because of its variable and evolving nature. Therefore, the various definitions of privacy differ according to the context, the people and the period of time.

[373] Electronic Privacy Information Center and Privacy International, 'Privacy and Human Rights – An International Survey of Privacy Laws and Developments' (2002) (Washington D.C. and London).
[374] For example, in Sweden the Swedish citizens are entitled to access the amount of tax paid by a person because of their tradition of open government while in United Kingdom and other European countries this information is considered private and not accessible to other citizens (Ian Wolden, 'Privacy and Data Protection' in Chris Reed, *Computer Law* (7th edn, Oxford University Press 2011) 573–626).

The concept of privacy is not only a privilege of our information age, but it has had a long-standing presence in history and in the cultures of nations for decades. During the Ancient and Classical Greek periods, for example, a private person was one who did not participate in public life – the term *'privatus'* in Latin meant 'a man holding no political office'.[375] At that time, most homes were windowless and people spent the majority of the day outdoors, on streets, in squares and in markets. Therefore, the term was used to emphasise the person's unwillingness or lack of capacity to participate in the political and social life of Athens, rather than to protect one's life from the public eye. The potential to invade privacy was limited because a person's life took place in public.[376]

In addition, the Eighth Commandment of the Old Testament (the Christian Bible) also deals with privacy under the concept of property rights ('You shall not steal').[377] The Eighth Commandment forbids the invasion of property and emphasises that theft is an act of violence against the private property of a person. Accordingly, the word *'property'* entails not only protection of physical objects but also protection of human life and body and protection of thoughts and feelings (protection of intellectual property). Thus, the Eighth Commandment provides individuals with the right to exercise complete control over who comes into their *territory* – their *privacy*.

Notwithstanding the different approaches to privacy through different periods of time, privacy as an independent legal value to protect a person's private life was developed only in the nineteenth century. As people's lives moved from the streets to behind the closed doors of their homes and offices, the potential to invade privacy was created along with the need to draw the line between individuals and their intruders (i.e. public actors, private actors or other individuals).

[375] WordSense.eu Dictionary, <http://www.wordsense.eu/privatus/> (accessed 8 August 2015).
[376] Savin (ed) 2013 (n 325) 190.
[377] George Z. Constandinides, 'The New Encyclopediko Dictionary of the Old Testament' (2nd edn, Publigations The Logos 1985) 201–202 (In Greek: Γεώργιου Ζ. Κωνσταντινίδη (Β' Έκδοση), '*ΝΕΟΝ ΕΓΚΥΚΛΟΠΑΙΔΙΚΟΝ ΛΕΞΙΚΟΝ ΑΓΙΑΣ ΓΡΑΦΗΣ*' (Εκδόσεις 'Ο Λόγος' 1985) 201–202); See also 'The Old Testament' in Today's Greek Version (Greek Publications 1997) 220–221 (In Greek: 'Η ΠΑΛΑΙΑ ΔΙΑΘΗΚΗ' (Έκδοση Ελληνικής Βιβλικής Εταιρείας 1997) 220–221).

In the modern age, there are various definitions that have been used to address the right of privacy. Privacy has been defined as the '*right to secrecy*' (the ability to keep something secret or to be kept secret from other people); the '*right to anonymity*' (the ability to be unknown, not to be identified); and the '*right to solitude*' (the ability to be alone, away from others).[378] In other words, privacy is the right of limited accessibility to a person and to information related to him/her. As Richard Parker stated, privacy is the 'control over when and by whom the various parts of us can be sensed by others'.[379]

Perhaps the most substantial and adapted view is that of Professors Samuel Warren and Louis Brandeis in their famous article *The Right to Privacy* in 1890 in which they proclaimed the need for a common law right to privacy – the 'right to be left alone'.[380] According to Warren and Brandeis, the need for legal protection emerged from the technological developments (portable photography equipment) and the business methods of the newspaper enterprises (yellow journalism) which enabled the recording, storing and distribution of previously private information of individuals in the public. They argued that the use of such devices and methods can lead to the invasion of the 'sacred precincts of private and domestic life'[381] and that not every aspect of a person's life that could be recorded should be allowed to be recorded and distributed.

Certainly, the above definitions draw the line between society and the freedom of the individual. From a legal point of view, the right to privacy provides individuals with a legal protection against any interference with their personal lives and enables them to exercise their freedoms (i.e. freedom to self-determination, to be different, to have different choices, etc.) and to create their own unique identities and individuality in order to participate in public and communicate with others.[382] Thus, the right of privacy is the *umbrella* for the protection of other fundamental values such as individual autonomy, integrity, self-determination, identity and dignity. As Daniel

[378] Routh E. Gavison, 'Privacy and the Limits of Law' (1980) Yale Law Journal 89(3) 421–471.
[379] Richard B. Parker, 'A Definition of Privacy' (1974) Rutgers Law Review 27 281.
[380] Warren and Brandeis 1890 (n 324).
[381] Warren and Brandeis 1890 (n 324).
[382] Hildebrandt, Gutwirth and Hert 2005, FIDIS Deliverable D7.4 (n 284) 18.

Solove explained, privacy is 'a plurality of different yet related things'.[383] Consequently, privacy is a diverse notion that encompasses four distinct but interrelated aspects:[384]

i. *Privacy of the Person* or *Bodily Privacy*. This is concerned with the integrity of the person's body and includes protection against unwanted physical intrusions or procedures (e.g. torture, medical treatments, blood tests, biometric measurements, etc.).
ii. *Privacy of Personal Data* or *Information Privacy*. Individuals must have the power to exercise control over the collection and use of their personal data as well as any decisions made based on those data (e.g. personal data and images). Such control helps individuals to 'build self-confidence' and 'to feel empowered'.[385]
iii. *Privacy of Personal Communications*. This includes the security and privacy of all forms of communication (e.g. telephone, email, virtual communications, face-to-face communications, etc.). Individuals must be free to communicate through the various forms of communication without being observed, monitored and/or recorded by other persons or organisations.
iv. *Territorial Privacy* or *Privacy of Personal Behaviour*. This aspect set the limits on unwanted intrusions into the person's private space whether in private places (e.g. home) or public places (e.g. work, shops etc.).

In this context, privacy has been evaluated as a fundamental human right, recognised by many international and regional treaties, and a reasonable expectation of every individual.

[383] Daniel Solove (ed), '*Understanding Privacy*' (Harvard University Press 2008) 9.
[384] Roger Clarke, 'What's 'Privacy'?' (2006) <http://www.rogerclarke.com/DV/Privacy.html> (accessed 10 July 2015); See also Ferretti 2009 (n 330); Finn, Wright and Friedewald 2013 (n 315) 3–32.
[385] Finn, Wright and Friedewald 2013 (n 315) 3–32.

3.6.2. Privacy as a Fundamental Human Right

Privacy is a fundamental, but not an absolute,[386] human right recognised in many international and regional treaties. The 1948 Universal Declaration of Human Rights (UDHR) provides protection against any interference with territorial and communication privacy. Specifically, Article 12 states that 'no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks'. Additionally, Article 17 of the 1966 International Covenant on Civil and Political Rights (ICCPR) is expressed in very similar wording.[387]

In Europe, the right to privacy is recognised and protected under the 1950 European Convention of Human Rights and Fundamental Freedoms (ECHR). After World War II, the Western European governments endorsed the approach that the protection of civil and political rights was necessary to pursue economic recovery and to guarantee peace in Europe. The dictatorship of Hitler and the fascist regime of the Nazis put the rights and freedoms of individuals in jeopardy and showed how easily such rights can be violated. Therefore, the governments of the Western states agreed that a list of human rights should be legally protected to limit governments from overstepping their authority against individuals' private domains.[388] The ECHR is the foundation for many legal instruments for the protection of human rights worldwide.

The most relevant provision of the ECHR for this thesis is Article 8 which entails a specific right related to individual privacy and constitutes the inspiration for the European data protection legislation. Article 8 provides that:

---

[386] Fundamental rights may be absolute or non-absolute rights. Absolute rights are the rights that cannot be restricted or suspended for any reason, even in circumstances of state emergency (e.g. right to protection from slavery and torture). Non-absolute rights are those which can be limited by the state according to the needs of the society.

[387] Article 17 of the ICCPR states: '(1) No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. (2) Everyone has the right to the protection of the law against such interference or attacks.'

[388] David P. Forsythe (ed), *'Human Rights in International Relations'* (Cambridge University Press 2000) 110.

> (1) Everyone has the right to respect for his private and family life, his home and his correspondence.
>
> (2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Although the term 'private life' is not further defined in the ECHR, there is no doubt that the protection of privacy is within the scope of Article 8(1). The term 'private life' has been broadly interpreted by the EU Commission (the 'Commission') and the European Court of Human Rights (the 'Court') to cover the rights of every individual to physical and moral integrity, to physical and social identity, to personal development, to autonomy and the right to establish relationships with other individuals in order to develop his/her own personality.[389] In relation to identity and autonomy, the Court deemed that identity is 'an essential condition of the right to autonomy and development' (*Pretty v. UK*[390]) and that it 'is within the inner core of the right to respect for one's private life' (*Odievre v. France*[391]). In this respect, privacy, autonomy and identity constitute related aspects that are protected under the scope of Article 8 of the ECHR.

Consequently, Article 8 does not only apply to matters of private nature (e.g. at home), but it also applies to matters of public nature such as relationships and interactions with others in public (e.g. business or professional activities).[392] This is because participation in public activities is part of the development of the identity

[389] *Niemitz v. Germany* App no 13710/88 (ECtHR, 16 December 1992); see also *Von Hannover v. Germany* App no 59320/00 (ECtHR, 24 June 2004), para 50; *X v. Iceland* App no 6825/74 (Commission decision 18 May 1976).
[390] *Pretty v. United Kingdom* App no 2346/02 (ECtHR, 29 April 2002).
[391] *Odievre v. France* App no 42326/98 (ECtHR, 13 February 2003).
[392] 'There appears, furthermore, to be no reason of principle why this understanding of the notion of "private life" should be taken to exclude activities of a professional or business nature since it is, after all, in the course of their working lives that the majority of people have a significant, if not the greatest, opportunity of developing relationships with the outside world.' (*Niemitz* v. *Germany* App no 13710/88 (ECtHR, 16 December 1992), para 29).

and the personality of every individual. The free establishment of relationships with others enables individuals to decide with which categories of people they are socially compatible and to which group they want to belong. In this way, individuals make decisions for their integrity and dignity within society.[393] Following this, private life is protected under Article 8 against intrusions by any person or organisation, whether of public or private nature (*Hatton v. UK*[394]).[395]

Furthermore, Article 8(2) provides positive and negative obligations upon public authorities in the sense that interference with the right to privacy is only permitted when the interference is 'in accordance with the law' and 'is necessary in a democratic society'. That is to say, any interference with the right must be authorised by law (national or international law) and must be based on fair, justified and legitimate reasons (proportionality principle)[396] and in the light of the moral values and needs of the society involved.

The EU Constitutional Law also protects the right to privacy under Article 7 of the Charter of Fundamental Rights of the European Union (the 'Charter').[397] The Charter is embedded in the Treaty of Lisbon (known as the EU Reform Treaty) and became a legally binding part of EU law, equal to the EU Treaties.[398] The text of the Charter replaced that of the Constitutional Treaty (known as the European Constitution). Certainly, therefore, the right to privacy continues to be protected as a fundamental principle of EU law.

Interestingly, the preamble of the Charter expressly states that the ECHR constituted a source of inspiration for the Charter itself and for this reason the Charter incorporates the rights in a similar way.[399] Therefore, the wording and interpretation

[393] Roosendaal 2013 (n 182) 82.
[394] *Hatton v. United Kingdom* App no 36022/97 (ECtHR, 8 July 2003), 15 BHRC 259.
[395] Ian J. Lloyd, '*Information Technology Law'* (6th edn, OUP 2011).
[396] Article 52(1) of the EU Charter provides that 'Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others'.
[397] Charter of Fundamental Rights of the European Union as proclaimed by the European Parliament, the Council and the Commission on 18th December 2000, OJ C 83, 30/03/2010 P. 389–403.
[398] Article 6(1) of the Lisbon Treaty.
[399] The preamble of the Charter states that: 'This Charter reaffirms, with due regard for the powers and tasks of the Community and the Union and the principle of subsidiarity, the rights as they result, in particular, from the

of Article 7 of the Charter follows that of Article 8 of the ECHR (the right to respect of private life).[400] The only difference regarding Article 7 of the Charter is the substitution of the word 'correspondence' with the word 'communications' in order to keep up with technological developments. In addition, the Charter also protects the right to human dignity,[401] the right to physical and mental integrity[402] and the right to individual autonomy (as it derives from the heading of Chapter I and the provisions of Article 1 to 5 of the Charter).

Arguably, the evaluation of privacy as a fundamental human right and its recognition by the ECHR had *prompted the trigger* for the development of the EU data protection legislation. In addition, the emergence of new advanced technologies and the processing of personal information, which involves many aspects of the individual's life, have created the need for legal protection of personal data – information privacy – and the balance of interests of all the parties involved.

3.7. The Genesis of Data Protection Legislation

In order to protect individuals' right to privacy, especially the right to informational privacy, it was indicated that precise and suitable rules for the protection of personal data were necessary. The national legislation of the Member States and Article 8 of the ECHR were not enough to provide adequate protection for the processing of personal data. The ECHR was adopted in 1950, before the threats that computer systems could pose to privacy were notable. In addition (despite the rulings of the Court that Article 8 applies to public and private sectors respectively), the primary purpose of Article 8 of the ECHR was to protect individuals against public and not

constitutional traditions and international obligations common to the Member States, the Treaty on European Union, the Community Treaties, the European Convention for the Protection of Human Rights and Fundamental Freedoms, the Social Charters adopted by the Community and by the Council of Europe and the case-law of the Court of Justice of the European Communities and of the European Court of Human Rights.'

[400] Article 52(3) of the Charter.

[401] Article 1: 'Human dignity is inviolable. It must be respected and protected'.

[402] Article 3: 'Everyone has the right to respect for his or her physical and mental integrity'.

private actors. Consequently, there was a need to set out rules that cover both sectors.[403]

This proposition was followed by two legal instruments that were drafted for the protection of personal data. First, the 1981 Convention of the Council of Europe ('Convention 108')[404] and second, the 1980 Organisation for Economic Cooperation and Development Guidelines (OECD).[405] Both instruments constitute a source of data protection law in many European states. The scope of the Convention 108 was to provide legal protection to individuals with regard to the processing of their personal data by both public and private entities. Its general aim was to protect privacy and to enable the free flow of data within the EU. In a similar way, the OECD adopted policy guidelines on the protection of personal data. Nevertheless, the principles provided by these legal instruments were in the form of recommendations (not obligatory) for the Member States. Thus, they allow Member States to decide independently as to how and to what extent to adopt these principles in their national law.

3.7.1. Data Protection as a Fundamental Right

Since the enactment of the Lisbon Treaty, the right to data protection is explicitly established at the EU constitutional level and thus is protected as a general principle of EU law. Article 16 TFEU (ex Article 286 TEC) states that 'everyone has the right to the protection of personal data concerning them' and it imposes the obligation of the European Parliament and the Council to establish laws for the protection of personal data.[406] In the same direction, the EU Charter, under the provisions of Article 8, specifically addresses the fundamental right to the protection of personal

[403] A.C. Evans, 'European Data Protection Law' (1981) AJCL 29 572.
[404] Convention for the Protection of Individuals Regarding to Automatic Processing of Personal Data, signed in Strasbourg on 28th January 1981.
[405] OECD Council Recommendations on the Protection of Privacy and Transborder Flows of Personal Data, 23 September 1980.
[406] Article 16(2) states that 'The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities'.

data and lays down specific guarantees for the processing of such data. Article 8 of the Charter provides that:

> (1) Everyone has the right to the protection of personal data concerning him or her.
>
> (2) Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which have been collected concerning him or her, and the right to have it rectified.
>
> (3) Compliance with these rules shall be subject to control by an independent authority.

Clearly, Article 8 of the Charter provides to data protection a status of autonomous fundamental right. In this way, it confirms its importance in the EU and distinguishes it from the fundamental right to privacy (which is protected under Article 7 of the Charter).

From the ECHR perspective, the Convention neither recognises the right to data protection nor does it provide any corresponding provision on the protection of personal data. Nonetheless, the Court has applied Article 8 of the ECHR (right to respect for private life) in order to give rise to the right to data protection. Based on the Court's rulings, the term 'private life' includes the protection of personal data (as defined by the DPD) and thus data protection falls within the scope of Article 8 of the ECHR (even though not all personal data are necessarily private[407]).[408]

[407] *Bavarian Lager* Case (n 10).
[408] *Amann v. Switzerland* App no 27798/95 (ECtHR, 16 February 2000), ECHR 2000-II, para 65; See also *Rotaru v. Romania* App no 28341/95 (ECtHR, 5 May 2000)), ECHR 2000-V, para 43; *M.M. v. United Kingdom* App no 24029/07 (ECtHR, 13 November 2012).

3.7.2. European Data Protection Directive 95/46/EC

Following, therefore, the remarkable increase in the amount of data processing, a more uniform solution, legally binding all Member States, has become necessary.[409] In this context, the European Parliament and the Council adopted, in 1995, the European Data Protection Directive 95/46/EC. The DPD was the first step of EU data protection legislation towards the protection of individuals' fundamental rights and values, especially the right to privacy. The two main elements of the DPD, which up until recently constituted the main legislative instrument for the protection of personal data in the EU, were the advanced technological developments and the need for free movement of data within the EU in order to eliminate barriers to trade and to e-commerce. Therefore, data protection was not only an issue of safeguarding individuals' right to privacy, but it was also an issue of economic importance.

The objective of the DPD is to protect individuals against unfair and unlawful collection and processing of their personal data, as well as to ensure respect for their right to privacy and for the free flow of personal data within the EU Internal Market.[410] This indicates, therefore, that the primary aim of the Directive is not merely to protect individuals' privacy, but also to serve and promote different social and economic interests. For this reason, the Directive has been continually criticised as to its effectiveness to provide adequate protection for individuals and their privacy.

Due to the challenges brought by new technologies, the vast amount of data in large databases and globalisation, the DPD has proven to be no longer efficient to protect individuals. As Gerrit Hornung said, the DPD 'appears to be an ancient regulatory instrument'[411] which needed to be reformed and modernised in order to ensure a high level of data protection. The extensive use of profiling technologies, the phenomenon of big data and the application of data mining techniques, although they create new opportunities for controllers to do business, also pose new threats to

[409] Evans 1981 (n 403) 572; See also Roosendaal 2013 (n 182) 88.
[410] Article 1 DPD.
[411] Gerrit Hornung, 'A General Data Protection Regulation for Europe? Light and Shade in the Commission's Draft of 25 January 2012 *Scripted (A Journal of Law, Technology and Society)* 9(1) 64.

individuals' rights and values, notably to privacy and data protection. All three factors enable controllers to obtain access to individuals' private lives while limiting individuals' abilities to control their personal data. Consequently, new technological developments create new legal challenges for data protection legislation that go beyond the ones considered under the DPD. Acknowledging, therefore, the new technological challenges and the threats to individuals' rights, in January 2012, the European Commission drafted the GDPR. The official text of the GDPR was published in the EU Official Journal on 4th May 2016 and it was enforced on 24th May 2016. It has been applied directly to all Member States since 25th May 2018.[412] The GDPR aims to modernise the current EU data protection legislation and to provide stronger, consistent and uniform rules for the protection of individuals' personal data and for the development of the Internal Market.[413]

3.7.3. The General Data Protection Regulation

Just like the DPD, the GDPR has two objectives: firstly, to reinforce the protection of individuals' fundamental rights and freedoms, in particular their right to the protection of personal data (both inside and outside the EU) and secondly, to strengthen the free movement of personal data in the Internal Market.[414] In doing so, the Regulation aims to enhance individuals' trust in the digital environment by providing them with more and effective control over their personal data, while, at the same time, intends to reinforce legal certainty by simplifying the legal environment for business entities through one single, uniform set of rules across all EU Member States, in order to promote the functioning of the Internal Market and to boost the digital economy, innovation and job creation in the EU.[415]

Having regarded the crucial role that data protection plays in the protection of fundamental rights and values of individuals, the following chapter will examine how profiling is regulated under the GDPR in order to determine how the EU data protection legislation protects these rights and values.

[412] Article 99 GDPR.
[413] Hustinx 2013 (n 3).
[414] Article 1 GDPR.
[415] Recital 7 GDPR.

Chapter 4

Regulating Profiling from a European Perspective

4.1. Introduction

The creation and application of profiles may affect individuals and their lives. This is because profiling enables business entities to discover new knowledge about their current or potential customers by creating new personal data about individuals, from data relating to other individuals (members of the group profiles to which the individuals belong), or even generating sensitive personal data from non-sensitive data. For example, by collecting customers' characteristics and past purchases relating to sexual behaviour in order to find their purchase habits, a business entity can infer (as probabilistic knowledge) if a certain customer is heterosexual or homosexual (information that the customers never provide to the business entity).[416] By attributing to individuals personal data which in fact belong to other individuals with whom they share some common characteristics (e.g. same purchases habits), there is a possibility to classify them in a category – profile – in which they do not belong. As a result, individuals are given new (incorrect) characteristics and values, based on which business entities decide whether to include or exclude them from certain services.

Consequently, the lack of transparency and accuracy that may result from these profiles can cause asymmetries of knowledge and unbalanced distribution of powers between controllers and individual subjects. As such, profiling challenges the protection of individuals' fundamental rights and values and creates conditions for surveillance, manipulation, threats to individuals' autonomy, discrimination, de-individuation, stigmatisation, stereotyping and inaccuracy in the decision process. In addition, the asymmetries of knowledge and the unbalanced distribution of powers

[416] Recommendation CM/Rec(2010)13 and Explanatory Memorandum on the Protection of Individuals with Regard to Automatic Processing of Personal Data in the Context of Profiling adopted by the Committee of Ministers of the Council of Europe on 23 November 2010 31.

are likely to affect the individuality of a person and the freedom to self-develop his/her own unique personality and identity within society, as well as to create potentials for classification, social sorting, social control and normalisation of individuals, either as customers or as citizens. Such potentials generate concerns over the individuals' autonomy and their right to self-determination.

It follows, therefore, that profiling poses challenges to the most basic principles of a democratic society and threatens individuals' fundamental rights to privacy and data protection. As a result, the challenges examined in Chapter 2 of this thesis exhibit the importance and the necessity of ensuring privacy and data protection rights and of questioning the applicability and effectiveness of the law to protect these rights within the context of profiling.

In order to protect individuals' rights to privacy and data protection, every business entity (controller) must comply with data protection legislation. The purpose of this chapter is to examine how profiling is regulated under the GDPR in order to determine how EU law deals with profiling and its challenges to the fundamental rights and values of individuals, notably to the rights to privacy and data protection.

The chapter is structured as follows: sections 4.2 and 4.3 focus on the objectives of the GDPR and emphasise the three most important changes to the new legislation. That is, the transition from Directive to Regulation (section 4.3.1), a new legal basis (section 4.3.2) and a new territorial scope (section 4.3.3). Section 4.4 deals with how profiling is regulated under the GDPR by examining the definition of profiling and the material and territorial scope of the Regulation; section 4.5 introduces the general data protection principles of the Regulation and examines how these principles are engaged with profiling; section 4.6 provides the criteria under which profiling is lawful for the scope of the Regulation; section 4.7 considers profiling on the basis of special categories of data and section 4.8 explores the specific rules for profiling by elaborating on the rights conferred to the individuals and the accountability of the controllers.

4.2. The General Data Protection Regulation

Just like the DPD, the GDPR has two objectives: firstly, to reinforce the protection of individuals' fundamental rights and freedoms, in particular their right to the protection of personal data (both inside and outside the EU) and secondly, to strengthen the free movement of personal data in the Internal Market.[417] In doing so, the Regulation aims to enhance individuals' trust in the digital environment by providing them with more and effective control over their personal data and, at the same time, intends to reinforce legal certainty by simplifying the legal environment for business entities through one single, uniform set of rules across all EU Member States in order to promote the functioning of the Internal Market and to boost the digital economy, innovation and job creation in the EU.[418]

It must be highlighted that, whereas the wording of the Directive designates the protection of the right to privacy as one of its objectives,[419] the wording of the Regulation does not expressly refer to the right to privacy itself but to the right to data protection.[420] Thus, the GDPR reflects the separation of the two rights and the proclamation of data protection as a distinct fundamental human right, under Article 8(1) of the Charter and Article 16(1) of the TFEU. Prima facie, this may suggest that the main objective of the GDPR is to protect the right to data protection and not the right to privacy. Nonetheless, in its preamble, the Regulation refers to the connection between the two rights by stating that the Regulation 'respects all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties, in particular the respect for private and family life, home and communications (…)'.[421]

It follows, therefore, that although the Regulation does not directly include the protection of privacy within its objectives, such protection is to be considered.

[417] Article 1 GDPR.
[418] Recital 7 GDPR.
[419] Article 1(1) DPD: 'In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy, with respect to the processing of personal data.'
[420] Article 1(2) GDPR: 'This Regulation protects the fundamental rights and freedoms of natural persons, and in particular their right to the protection of personal data.'
[421] Recital 4 GDPR.

However, it should be noted that the preamble of an EU legislation (in this case of the GDPR) has no binding legal force and cannot be relied on as a ground for derogating from the actual provisions of the legislation in question, even though, in practice, the Courts may use the explanation given in the preamble to interpret its provisions.[422] Arguably, it is not clear whether the wording of Recital 4 is sufficient to provide (effective) protection to the right to privacy under the Regulation for the moment. This issue will be clarified more in the process of time depending on the extent to which the Courts will make use of the wording of Recital 4 when deciding the cases to be brought before them.

4.3. Changes of Emphasis

Before analysing the provisions of the Regulation concerning profiling, it is useful to refer to the three most important changes to the new data protection legislation.

4.3.1. From Directive to Regulation: A Uniform Level of Protection

The first most important change to the new data protection legislation is the transition from Directive to Regulation in order for the new legal instrument to better serve the goal of a uniform level of data protection in Europe. Although one of the objectives of the DPD was to achieve an equivalent high level of protection within the EU Member States, this objective has not materialised. The result is rather the existence of a considerable divergence between the national data protection legislations, which has ended in legal uncertainty and different levels of protection for individuals and causes unnecessary costs and administrative obligations for controllers.[423] Perhaps the best example of this legal differentiation is the implementation of the definition of *personal data* in the UK. The Court of Appeal has limited the scope of data protection legislation by adopting a more restrictive

[422] *CJEU 19 November 1998, C-162/97 (Nilsson, Hagelgren and Arrborn)* para. 54; See also Tadas Klimas and Jūratė Vaičiukaitė, *'The Law of Recitals in European Community Legislation'* (2008) ILSA Journal of International & Comparative Law (1) 92.

[423] Viviane Reding, 'The European Data Protection Framework for the Twenty-First Century' (2012) International Data Privacy Law 2(3) 121; See also Peter Blume, 'Symposium on EU Data Protection Reform: The Myths Pertaining to the Proposed General Data Protection Regulation' (2014) International Data Privacy Law 1.

interpretation of personal data (*Durant v. FSA*).[424] In this way, the UK's interpretation clashes with the EU's broad understanding of personal data as given not only by the Article 29 Working Party,[425] but also by the ECJ.[426]

In accordance with Article 288 TFEU, a 'Directive' is binding to (any one or all) Member States as to the goal to be achieved, while leaving the choice to the Member States as to the form and method to be adopted in order to achieve that goal.[427] In other words, a 'Directive' binds the Member States as to the result but not as to the method used to achieve the result. In this way, the DPD renders a degree of flexibility to the Member States on how to adopt its provisions in their national legislations. On the contrary, a 'Regulation' is binding and directly applicable to all Member States without requiring any further procedure or implementation.[428] Therefore, a 'Regulation' is considered to be a more convenient and drastic legal instrument for the elimination of the legal diversity between national laws and the setting of more uniform data protection rules across the EU. According to the Commission, such uniform rules will reduce legal fragmentation, provide greater legal certainty, ensure a more effective level of protection for individuals and promote the development of the Internal Market by reducing the cost and the administrative obligations of the controllers.[429]

---

[424] In *Durant* the appellant requested the disclosure of bank records which contained his name. The Court of Appeal ruled that the 'mere mention of the data subject in a document held by a controller does not necessarily amount to personal data' and narrowed the meaning of personal data to data that concern biographical information about the data subject or data that has the data subject as its focus (*Durant v Financial Services Authority* [2003] EWCA Civ 1746, para. 28).

[425] Article 29 Working Party, 'Opinion No. 4/2007 on the Concept of Personal Data', adopted on 20th June 2007 (01248/07/EN, WP 136); See also Article 29 Data Protection Working Party, Working Document on Data Protection Issues Related to RFID Technologies, 19 January 2005 (10107/05/EN, WP 105) 8.

[426] In the case of *Bodil Lindqvist* the ECJ examined the meaning of personal data in relation to information uploaded to a website and ruled that the term personal data 'undoubtedly covers the name of a person in conjunction with his telephone co-ordinates or information about his working conditions or hobbies' (CJEU 6 November 2003, C-101/01 (*Lindqvist*,) para. 24, 25, 27).

[427] Article 288 TFEU (ex Article 249 TEC) states: 'To exercise the Union's competences, the institutions shall adopt regulations, directives, decisions, recommendations and opinions. A regulation shall have general application. It shall be binding in its entirety and directly applicable in all Member States. A directive shall be binding, as to the result to be achieved, upon each Member State to which it is addressed, but shall leave to the national authorities the choice of form and methods. A decision shall be binding in its entirety. A decision which specifies those to whom it is addressed shall be binding only on them. Recommendations and opinions shall have no binding force.'; See also Paul Craig and Grainne de Burca, *EU Law: Text, Cases, and Materials* (2nd edn, Oxford University Press 1998) 106–108.

[428] Craig and Burca 1998 (n 427) 106–108.

[429] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: 'Safeguarding Privacy in a Connected World: A European Data Protection Framework for the 21st Century', COM (2012) 9 final, 25/01/2012.

However, it should be noted that the direct applicability of a 'Regulation' does not prohibit the Member States from adopting additional legal measures in order to ensure their compliance with its provisions, especially when the 'Regulation' itself provides for such an obligation.[430] For example, the GDPR allows Member States to adopt measures to deal with certain situations, such as the processing of genetic or biometric data or data concerning health or children.[431]

This indicates that the Member States will still have a degree of flexibility to decide what kind of legal measures to adopt in their national legislations in order to ensure the application of the provisions of the GDPR, although of course within its limits. Consequently, some degree of diversity is to be expected. As Christopher Kuner has stated, 'even a regulation cannot result in complete, 100% harmonization of all legal provisions affecting data protection or totally eliminate the need to amend national laws'.[432] What remains to be seen, however, is the degree to which such diversity will occur and how it may or may not influence the effective applicability of the GDPR, especially in the context of profiling.

4.3.2. A New Legal Basis

A second change of emphasis is the new legal basis for the adoption of the GDPR. As mentioned in Chapter 3 of this thesis, since the enactment of the Lisbon Treaty, the right to data protection is explicitly established at the EU constitutional level under Article 16 TFEU and thus is protected as a general principle of EU law.[433] As a result, Article 16 TFEU introduces a new legal basis for the adoption of EU data protection legislation. Following this development, Recital 12 states that the legal basis of the Regulation is Article 16(2) TFEU, which provides the adoption of rules (by the European Parliament and the Council) relating to the protection of individuals with regard to the processing of personal data and rules relating to the free movement of such data. Clearly, there is a significant difference between the

[430] Reding 2012 (n 428) 121
[431] Article 9(4) GDPR.
[432] Christopher Kuner, 'The European Commission's Proposal Data Protection Regulation: A Copernican Revolution in European Data Protection Law' (2012) Bloomberg BNA Privacy and Security Law Report 4.
[433] See section 3.7.1 in Ch 3.

scopes of the two legal instruments.

While the legal basis of the DPD, under Article 100a EC Treaty (now Article 114 TFEU (ex Article 95 TEC)), authorises the adoption of legal measures for the establishment and functioning of the Internal Market, the legal basis provided under Article 16(2) TFEU authorises the adoption of rules not only for the free movement of personal data but also for the protection of individuals with regard to the processing of their personal data. This means that the wording of Article 16(2) TFEU exceeds the scope of Article 100a EC Treaty in the sense that it goes beyond the aim of the functioning of the Internal Market and requires the EU institutions to also adopt rules for the protection of individuals.[434]

4.3.3. Territorial Scope

The third aspect that differentiates the GDPR from the DPD is the changes made with regard to the territorial scope of the Regulation. Article 3 GDPR provides that the Regulation applies not only to the processing of personal data involving controllers or processors[435] established in the EU, but also to controllers or processors not established in the EU if their processing activities involve 'the offering of goods and services' to data subjects in the EU or 'the monitoring of the behaviour' of such data subjects.[436] In this respect, Article 3 GDPR extends the territorial scope of the Regulation and makes it more flexible than the scope of Article 4 DPD which limits the applicability of the Directive to non-EU controllers, unless such controllers are making use of processing equipment that is situated in the EU.[437] In relation to data subjects, the applicability of the Regulation is limited only to individuals residing in the EU, although it is not clear whether such residence

[434] Hustinx 2013 (n 3) 19.
[435] '"controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law' (Article 4(7) GDPR); '"processor" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller' (Article 4(8) GDPR).
[436] A further explanation of the terms 'offering of goods and services to' and 'the monitoring of the behaviour of' data subjects in the EU is further provided in section 4.4.2.2 of this chapter; See also Recital 23 and 24 GDPR.
[437] Savin (ed) 2013 (n 325) 207.

must be permanent or whether a temporary residence will suffice.[438] Such limitation, however, is arguable bearing in mind that the preamble of the Regulation states that the protection provided under the Regulation concerns natural persons, 'whatever their nationality or place of residence'.[439]

All of the aforesaid three changes create a feeling of innovation and give the idea that the new data protection legislation intends to adopt a very different approach to that of the DPD by adopting more modernised, globalised and uniform principles for the protection of personal data in the context of profiling. The actual effectiveness of the new data protection legislation, however, can only be determined by examining the degree to which the provisions of the GDPR achieve its respective objectives in relation to profiling. The next sections, therefore, examine how the provisions of the GDPR regulate profiling.

4.4. Regulating Profiling under the GDPR

Up until recently, EU data protection legislation had not provided an explicit definition of the term *profiling* nor had it included any reference to the word profiling. The DPD only provides rules for the processing of personal data in general. The only provision that could be seen to deal with profiling is Article 15 DPD.[440]

Article 15 DPD provides the right for every person not to be subject to a decision based solely on the automated processing of data intended to evaluate personal aspects relating to him/her, unless such a decision is taken in the course of entering into or of performance of a contract, or is authorised by law.[441] The primary focus of

[438] Kuner 2012 (n 432) 4.
[439] Recitals 2 and 14 GDPR; See also Kuner 2012 (n 432) 4.
[440] It should be noted that the e-Privacy Directive 2002/58/EC as it was amended by the Directive 2009/136/EC, although it does not explicitly refer to profiling, allows the use of cookies and other tracking devices that can be used for profiling activities where the controller has informed the user about the purpose of profiling and where he/she has obtained the user's consent (Article 5(3)).
[441] Article 15(1) DPD: 'Member states shall grant the right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability or conduct etc.'

this article is on the 'automatisation of decisions about individuals'[442] resulting from the processing of their data. The article does not create a direct prohibition on a particular type of decision-making, but rather it confers to individuals a right to prevent them from being subjected to automated decision-makings.[443] Therefore, decisions based on profiling are considered to be within the scope of Article 15 DPD to the extent that there is no human involvement in the process (decisions should be based entirely on the results produced by the profile).[444] One of the problematic aspects of Article 15 DPD is that it is only applied to the application of the profiles (decision-making process) and not to the process of creating the profiles. Thus, the DPD did not regulate the creation of profiles but only set out restrictions on the way those profiles are to be used.

For this reason, the Regulation attempts to strengthen the protection of individuals in relation to profiling by regulating not only the decision-making resulting from the application of the profiles but also the creation of the profiles.[445] In this respect, the Regulation sets out specific rules for profiling and indicates that the processing of data for profiling purposes is subject to the data protection principles under Article 5 GDPR and the provisions regulating the lawfulness of the processing under Article 6 GDPR (section 4.8 analyses the specific rules for profiling and sections 4.5 and 4.6 analyse, respectively, data protection principles and the legal basis for profiling).[446] Additionally, Article 4(4) GDPR provides an explicit definition of profiling. In this way, the Regulation affirms that the processing of personal data for profiling is undoubtedly subject to the scope of the new data protection legislation.

4.4.1. Defining Profiling

Profiling is defined in Article 4(4) of the Regulation as:

[442] Lee Bygrave, 'Automated Profiling – Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling' (2001) Computer Law & Security Report 17(1) 18.
[443] Bygrave 2001 (n 442) 17.
[444] Article 15 DPD is closely related to the rights conferred under Articles 10, 11 and 12 of the DPD which provide to individuals the rights to be informed for the collection of their personal data and to obtain knowledge of the logic involved in any processing of such data, in particular in the case of automated decision-makings.
[445] Vermeulen 2013 (n 123).
[446] Recital 72 GDPR.

> 'any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;'

According to the above definition, profiling consists of two elements: (a) the processing of data to evaluate certain personal aspects – the *creation of profiles* – and (b) the analysis or prediction of an individual's aspects – the *application of profiles*.[447] This can also be affirmed by the wording of Recital 60 which states that the data subject should be informed of the existence of profiling (meaning the creation of a profile) and the consequences of such profiling (meaning the application of a profile).

In addition, Recital 71 states that an individual should have the right not to be subject to an automatic decision 'which may include a measure, evaluating personal aspects (…)' relating to him/her. A *decision* requires that a judgement is made after some consideration.[448] A *measure*, on the other hand, involves any course of action that is taken to come to a particular outcome (that action could be a decision).[449] In explaining the extensive scope of the term *measure*, the EU former Commissioner Viviane Reding gave the example of targeted marketing for cancer drugs: 'the targeted marketing of specific medical products against cancer based on the search made by an individual on the internet would fall under this concept of "measure"'.[450] In this way, therefore, the Regulation expands the scope of data protection legislation to protect individuals not only against the *application* – *decisions* – but also against the *creation* of profiles intending to evaluate personal aspects relating to them.

---

[447] Hildebrandt 2008b (n 23) 17.
[448] Harald Ofstad, *An Inquiry into the Freedom of the Decision* (Norwegian University Press 1961) 15.
[449] Vermeulen 2013 (n 123) 8.
[450] Viviane Reding, 'The EU Data Protection Regulation: Promoting Technological Innovation and Safeguarding Citizens' Rights' European Commission (SPEECH/14/175, 4 March 2014) <http://europa.eu/rapid/press-release_SPEECH-14-175_en.htm?locale=en> (accessed 20 April 2016).

4.4.2. When Does Profiling Fall Within the Scope of the GDPR?

In order to determine when data protection legislation is applicable to profiling, it is necessary to examine the conditions under which the GDPR applies. For this reason, therefore, it is necessary to examine the material and territorial scope of the Regulation.

4.4.2.1. Material Scope of the Regulation

As it is derived from the definition of profiling, for the Regulation to be applied, profiling must involve the processing of personal data. Thereby, the two principal elements of data protection legislation are the terms *personal data* and *processing*. The first question, therefore, is whether the processing of data using profiling technologies constitutes processing within the meaning of the Regulation.

The Regulation applies when personal data are 'wholly or partly processed by automatic means'.[451] The only exception for manual processing is where the processing is part of a filing system.[452] Under Article 4(2) GDPR, 'processing' is defined as 'any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automatic means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction'.[453] In a broad sense, therefore, even the slightest collection and use of personal data constitutes a processing activity within the scope of the Regulation.[454] This broad approach has been confirmed by the ECJ in the case of *Lindqvist*.[455] The ECJ agreed with the

[451] Article 2(1) GDPR: 'This Regulation applies to the processing of personal data wholly or partly by automatic means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system'.
[452] Article 4(6) GDPR: 'filing system' means any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis'.
[453] This is similar to the DPD definition except that the GDPR incorporates three additional elements: 'sets of personal data', 'structuring' and 'restriction'.
[454] Article 2(2) GDPR covers the conditions under which the processing of personal data is not subject to the scope of the Regulation and Article 2(3) GDPR provides that the processing of personal data by EU institutions, bodies, offices and agencies is subject to the rules of the Regulation.
[455] *Lindqvist* Case (n 426).

Swedish government's argument that 'as soon as personal data are processed by a computer, whether using a word-processing programme or in order to put them on an internet page, they have been the subject of processing'.[456]

Following the above analysis and considering that: (a) a mere collection and use of personal data constitutes a processing activity under the Regulation; (b) profiling, by definition, requires the *use* of data (to evaluate, analyse or predict individuals' personal aspects); and (c) profiling, as it is shown from the findings of the first chapter, involves the collection, recording, dissemination, combination and categorisation of individuals' data (in profiles), it is to be concluded that profiling constitutes a form of automated processing activity within the meaning of the Regulation.

The second question which arises is whether the data being processed by profiling technologies constitute personal data within the meaning of the Regulation. *Personal data* is defined in Article 4(1) GDPR as 'any information relating to an identified or identifiable natural person ('data subject') (…)'. Thus, the definition of personal data includes four elements: 'any information', 'relating to', 'an identified or identifiable' and 'natural person'. Together, all four elements assess whether the data processed constitute personal data and whether data protection legislation should apply. These elements have been examined by the Article 29 Working Party in the context of interpreting the definition of personal data under the DPD.[457]

1. 'Any Information' and 'Relating to'

'Any information' means any form of data without limitations to content or to technology as long as the data can be used as a link to identify the individual subject. It includes texts, videos, images, voices, fingerprints, genetic or biometric data and so on.[458] In other words, personal data can refer to both objective (e.g. colour of

[456] *Lindqvist* Case (n 426) para 21.
[457] Article 29 Working Party, Opinion No. 4/2007 (425); See also Article 29 Data Protection Working Party, 10107/05/EN, WP 105 (n 425) 8.
[458] Article 29 Working Party, Opinion No. 4/2007 (n 425) 7; It should be added that, for the purpose of this thesis, where the provisions of the GDPR are similar to those under the DPD, the rulings of the EU Courts and

eyes, type of blood etc.) and subjective (e.g. opinions, judgements, beliefs etc.) information about the individual.[459] The term 'relating to' includes any data which refer to the identity, characteristics or behaviour of an individual or which are used to determine or influence the way in which that individual is treated or evaluated, regardless of his/her 'position or capacity (as a customer, patient, employee, etc.)'.[460] According to the Article 29 Working Party, in order to consider if data are related to a particular individual one of the following three elements should be justified: *content*, *purpose* or *result*.[461]

As appears from the analysis below, profiling fulfils all of the aforesaid three elements. The *content* element is justified if the data are about the individual.[462] Profiling uses data relating to individuals' aspects (e.g. an individual's medical or employment records). The *purpose* element is satisfied when the data are used or intended to be used to determine the manner in which the individual's behaviour is treated, influenced or evaluated.[463] Profiling enables the creation of profiles[464] with the intention of evaluating, analysing or predicting individuals' behaviour (e.g. the purpose of an employer is to detect fraudulent activities by his/her employees, or the purpose of a doctor is to evaluate or predict the effectiveness of a treatment for his/her patient). Finally, a *result* element is present when the processing of data is likely to affect the rights and interests of the individual.[465] In other words, the term 'any information relating to data subject' does not only encompass data that refer to the identity, characteristics or behaviour of an individual but also to data that could facilitate different treatments among the individuals. Profiling involves a *result* element because it enables the making of decisions about individuals that may affect

---

the recommendations and opinions of the Article 29 Working Party concerning the provisions of the Directive are to be considered relevant (unless the EU Courts or the Board decide otherwise) and thus be used for the interpretation and further clarification of the provisions of the Regulation.

[459] Jacob Kohnstamm, 'Privacy By Debate: The European Data Protection Supervisor's Contribution to Collaboration Between National Data Protection Authorities' in Hielke Hijmans and Herke Kranenborg (eds), *Data Protection Anno 2014: How to Restore Trust? Peter Hustinx, European Data Protection Supervisor (2004-2014)* (Cambridge: Intersentia Publishing Ltd. 2014) 153; See also Antoinette Rouvroy, 'Privacy, Data Protection, and the Unprecedented Challenges of Ambient Intelligence' (2008) Studies in Ethics, Law, Technology 2(1) 11.

[460] Article 29 Working Party, Opinion No. 4/2007 (n 425) 7.

[461] Article 29 Working Party, Opinion No. 4/2007 (n 425) 10.

[462] Article 29 Working Party, Opinion No. 4/2007 (n 425) 10.

[463] Article 29 Working Party, Opinion No. 4/2007 (n 425) 10.

[464] 'Profile' is 'a set of data characterising a category of individuals that is indented to be applied to an individual' (Recommendation CM/Rec (2010)13 (n 416) Article 1(d)).

[465] Article 29 Working Party, Opinion No. 4/2007 (n 425) 11.

their rights and their future opportunities (e.g. treating an employee differently from his/her colleagues as a result of his/her profile may affect his/her rights to equality and non-discrimination within the employment context).

2. 'Identifiability' and 'Natural Person'

Like the DPD, the GDPR applies to an identified or identifiable natural person. An 'identified or identifiable natural person' means that the personal data are the data of a natural and not of a legal person. In other words, the Regulation applies only to identified or identifiable alive persons and it excludes from its scope the protection of corporate data and trade secrets.[466]

A person is considered to be identified if, within a group of people, that person is distinguished (singled out) from all other members of the group (e.g. the collected data are directly related to a named individual).[467] An identifiable individual is one who can possibly be distinguished within a group of people (e.g. the collected data do not enable the identification of a particular individual unless additional data are collected about that individual).[468] In other words, an identifiable individual is one who can possibly be identified, directly or indirectly, based on certain identifiers.[469]

A new aspect of the Regulation is that Article 4(1) GDPR considers identifiers such as names, identification numbers,[470] location data or data related to physical, physiological, genetic, mental, economic, cultural or social identity, as well as online identifiers (IP addresses, cookies or RFID-tags) to be personal data. In addition, Recital 30 states that online identifiers may allow the indirect identification of an individual because when combined with unique identifiers they can be used to create profiles about individuals and thus enable individuals to be singled out even when

[466] Savin (ed) 2013 (n 325) 196.
[467] Article 29 Working Party, Opinion No. 4/2007 (n 425) 12.
[468] Ronald Leenes, 'Do They Know Me? Deconstruction Identifiably' (2007) University of Ottawa Law & Technology Journal 4(1-2) 139.
[469] Recital 26 GDPR.
[470] For the processing of national identification numbers (or any other identifier of general application) the Regulation requires that such processing should only take place if the controller adopts appropriate safeguards for the rights and freedoms of individuals and obliges Member States to specify the conditions for such processing (Article 87 GDPR).

their real names are not known.

In this way, the Regulation states that profiling might affect individuals even if they are not identified by their names but rather they are recognised by their devices.[471] For example, an online retailer places a cookie on a customer's computer when the customer first visits its website in order to track his/her movements (e.g. what products he/she viewed, at what price etc.) during his/her presence on the website and creates his/her profile. The cookie allows the retailer to recognise the customer every time he/she visits the website because of the data he/she provides to the website (e.g. username and product of preference). The retailer does not know the real name of the customer (unless the customer provides it). However, the cookie also enables the retailer to track the customer's movements on different websites and thus to collect additional data (e.g. location, music preferences, employment status etc.) about the customer which can reveal his/her identity within the meaning of the Regulation.

Thus, profiling technologies allow the collection of data relating to individuals' activities, behaviour and preferences which can directly or indirectly be linked to the individuals' identities. Consequently, the data collected by profiling technologies can be considered as data relating to an identified individual according to the interpretation of the Article 29 Working Party and, in this respect, constitute personal data within the meaning of the Regulation.

It should be added that anonymous data[472] are excluded from the scope of the data protection legislation while pseudonymous data (e.g. online identifiers such as online traces), although not directly identifiable, constitute personal data under the Regulation because an individual can still be identified with the use of additional

[471] Luiz Costa and Yves Poulet, 'Privacy and the Regulation of 2012' (2012) Computer Law & Security Review (3) 255.
[472] Recital 26 GDPR defines anonymous data as 'information which does not relate to an identified or identifiable natural person or personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable'.

data.[473]

The key issue for identification is whether it is possible to identify an individual and not whether the identification will actually take place.[474] Therefore, the possibility that a controller will be able to identify an individual is to be determined according to the test of reasonableness: whether the steps taken by the controller (e.g. time, money, effort, technology used for processing and technological developments) are reasonable for the identification of the individual in question.[475] If the steps taken are reasonable (e.g. no disproportionate effort was needed), the data are considered to be the personal data of an identified or identifiable person.

4.4.2.2. Territorial Scope of the GDPR

Having demonstrated that profiling activities involve the processing of personal data, the next question is whether a profiling activity falls within the territorial scope of the Regulation. As previously mentioned, the Regulation expands its territorial scope not only to controllers or processors established in the EU, but also to controllers or processors not established in the EU if they offer goods or services to or monitor EU data subjects. This means that business entities which are not established in the EU, but which are involved in profiling concerning EU data subjects, will still be subject to the scope of the Regulation (including profiling for marketing purposes).

In the case of EU controllers or processors, the Regulation applies when the processing of data takes place in the context of the activities of an establishment of the controller or processor in the EU.[476] According to Recital 22, an establishment of the controller constitutes the place of 'the effective and real exercise of activity through stable arrangements'. The legal form of the establishment is not the

[473] Article 4(5) GDPR: '"pseudonymisation" means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person'.
[474] FIDIS consortium, 'D7.16: Profiling in Financial Institutions' (FIDIS 29 June 2009) <http://www.fidis.net/> (accessed 14 July 2014).
[475] Recital 26 GDPR: '(…) To determine whether a natural person is identifiable account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly (…)'; See also Hornung 2012 (n 411) 69.
[476] Article 3(1) GDPR.

determining factor (e.g. whether a branch or an office). Moreover, the processing of data itself does not necessarily have to take place in that location. In its decision in the case of *Weltimmo*, the CJEC ruled that in order to determine if a business entity has an establishment in a Member State, 'the degree of stability of the arrangements and the effective exercise of activities in that other Member State must be interpreted in the light of the specific nature of the economic activities and the provision of services concerned'.[477]

The Court also held that the presence of only one representative of the business entity can suffice to constitute a stable arrangement, if that representative acts with a sufficient degree of stability through the presence of the necessary equipment for provision of the specific services of the business entity. In addition, the Court in *Google Spain* ruled that a processing activity is considered to be carried out in the context of the activities of an establishment when the activities of a business entity are inextricably linked to the activities of its establishment.[478]

In relation to non-EU controllers and processors, the Regulation applies where one of the following two conditions is present: (a) the processing activity is related to offering goods or services to data subjects who are in the EU, irrespective of whether there is a payment; or (b) the processing activity is related to the monitoring of the behaviour of such data subjects as far as their behaviour takes place within the EU.[479]

In order to determine if the non-EU controller or processor is offering goods or services to data subjects in the EU, it should be established that the controller or processor is envisaging the offering of goods or services to data subjects in one or more EU Member States.[480] In other words, it should be examined whether the business entity has the intention to offer its goods or services to individuals in the EU. For example, it should be examined whether the business entity offers its services in a language or in a currency generally used in the EU or whether it uses

[477] CJEU 1 October 2015, C-230/14 (*Weltimmo*) para. 28–30.
[478] CJEU 13 May 2014, C-131/12 (*Google Spain v Costeja González*) para. 56.
[479] Article 3(2) GDPR.
[480] Recital 23 GDPR.

the language or the currency of the place of its establishment. Whereas in the first case there is a sufficient intention to offer the services to individuals in the EU, in the second case the use of a non-EU language or currency is insufficient to prove such intention.

Also, in order to determine if a processing activity of a non-EU controller or processor is monitoring the behaviour of a data subject (in the EU), it should be examined whether such a controller or processor is tracking individuals on the Internet. The Regulation provides that such tracking must include 'potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes'.[481] Thus, monitoring an individual's behaviour involves a profiling activity (which consists of the creation of a profile and the intention to apply this profile).

Therefore, any non-EU business entity which is involved in the processing of personal data of EU residents, with the intention to create and apply a profile to them, is subject to the rules of the Regulation. For example, a business entity based in Dubai that collects personal data of EU shoppers through the use of cookies, with the intention to profile them according to their purchase habits, is subject to the rules of the Regulation because the data collected (e.g. product and price preferences) are related to profiling (monitoring of behaviour).

The result of this new territorial regime is that many non-EU business entities which are engaged in profiling, either by offering their goods and services over the Internet to individuals residing in the EU or by monitoring such individuals' behaviour, are subject to the rules of the GDPR.

[481] Recital 24 GDPR.

4.5. Data Protection Principles

As it is stated above, a novelty in the GDPR is the fact that Recital 72 states that profiling is subject to data protection principles and the rules governing the legal basis for the processing of data. Therefore, having examined the conditions under which profiling is subject to the rules of the EU data protection legislation, the following section will examine how the general principles of the Regulation engage with profiling.

The Regulation creates rights and responsibilities from the moment personal data are collected and processed.[482] Article 5 GDPR (which corresponds to Article 6 DPD) defines a number of general principles which regulate the lawfulness of the collection and processing of personal data. According to its provisions, personal data must be:

> '(a) processed lawfully, fairly and in a transparent manner (…) ('lawfulness, fairness and transparency');
> (b) Collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes (…) ('purpose limitation');
> (c) adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation' principle);
> (d) accurate and kept up to date (…) ('accuracy');
> (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed (…) ('storage limitation');
> (f) processed in a manner that ensures appropriate security of the personal data (…) ('integrity and confidentiality')'.[483]

[482] Wim Schreur et al., 'Cogitas, Ergo Sum. The Role of data protection and Non-Discrimination Law in Group Profiling in the Private Sector' in Mireille Hildebrandt and Serge Gutwirth (eds), *Profiling the European Citizen: Cross-Disciplinary Perspectives* (Springer 2008) 243.
[483] Article 5(1) GDPR.

In addition, Article 5(2) GDPR strengthens the accountability and liability of the controllers in the processing of personal data by providing that they must be 'responsible for, and be able to demonstrate compliance with' the above principles ('accountability').

4.5.1. Fairness and Transparency

The goal of fairness and transparency principles is to minimise the privacy risks raised by the disclosure and (re-) use of personal data, by giving individuals the right to control their personal data.[484] Both principles demand that the processing of personal data should be compatible with the individual's understanding of how his/her data must be processed, unless there is a legitimate compelling interest in other or further processing.[485]

In this respect, both principles require that individuals must obtain knowledge of the fact that data concerning them are collected and intended to be processed and for what purpose.[486] They also require that individuals should be made aware of their rights provided under the Regulation, as well as any risks associated with the processing of their personal data.[487]

This means that a profiling activity is fair and transparent only if the individuals are informed (in clear and plain language), at the time of the collection, of the collection and processing of their data, the purpose of profiling and of the consequences of such profiling on them. To ensure, therefore, the fairness and transparency of profiling, the Regulation strengthens the obligations for controllers to adopt clear and accessible policies, to keep records of their profiling activities and to inform individuals about the processing of their data, including the existence of profiling, and to give them notice in case of breach of their data, as well as to enable them to

[484] Culnan and Armstrong 1999 (n 318) 107.
[485] U.S. Information Infrastructure Task Force (IITF), 'Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information' (1995) Washington, DC: Department of Commerce).
[486] Costa and Poulet 2012 (n 471) 256; See also Article 29 Working Party, 'Opinion No. 8/2014 16 on the Recent Developments on the Internet of Things' adopted on 16th September 2014 (14/EN/WP 223).
[487] Recital 39 GDPR.

exercise their rights.[488] In addition, the Regulation provides to individuals a set of data protection rights that enable them to have access to and exercise control over their personal data (for further elaboration on these rights please see sections 4.8.1 to 4.8.4).

4.5.2. Purpose Limitation

The purpose limitation principle plays a pivotal role in data protection legislation. In a similar way to the DPD,[489] the Regulation provides that the processing of personal data can only take place for the specific purpose for which the data are collected and that such purpose must be determined at the time of the collection.[490] Thus, business entities should explicitly specify the purpose for which they intend to use profiling before the collection of the data. The main goal of this principle is to ensure that the processing of data is lawful, fair and transparent. The re-processing of data for other purposes is prohibited unless such further purposes are compatible with the purpose the data have been collected for in the first place.

As in the case of the DPD, the term *compatible* is not further defined. However, a new element of the Regulation is that it introduces a list of factors under which the controller can determine whether the processing for other purposes is compatible with the purpose for which the data are initially collected.[491] In this way, the Regulation allows for a broad interpretation of the term 'compatible' and thus creates for controllers the flexibility to process data for *any* other purposes which may be

[488] Article 12 GDPR provides that the controllers must adopt 'transparent, intelligible and easily accessible' policies in order to allow individuals to exercise their rights as well as to communicate any information provided under Articles 13–22 and 34 GDPR. In addition, Recital 58 GDPR requires that '(…) any information addressed to the public or to the data subject be concise easily accessible and easy to understand, and that clear and plain language and, additionally, where appropriate, visualisation be used (…)'; See also sections 4.8.5 to 4.8.9 of this chapter for a detailed analysis on the obligations of controllers.

[489] Article 6(1)(b) DPD requires that personal data must be 'collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards'.

[490] Recital 39 GDPR; See also Article 29 Working Party, 'Opinion No. 03/2013 on Purpose Limitation' adopted 2nd April 2013 (00569/13/EN WP 203) 15.

[491] Article 6(4) and Recital 50 GDPR and state that the controller must take into account: (a) any link between the initial purposes and the purposes of the intended further processing; (b) the context in which the personal data have been collected and the reasonable expectations of individuals based on their relationship with the controller; (c) the nature of the personal data; the consequences of the intended further processing for individuals; and (d) the existence of appropriate safeguards (e.g. encryption or pseudonymisation); See also the Article 29 Working Party, Opinion No. 03/2013 (n 490).

considered compatible with their initial profiling activities.

Such incompatible processing could create uncertainty for the individuals and make profiling unlawful, unfair and non-transparent. However, the Regulation attempts to restrict such flexibility by setting out two conditions under which the further use of personal data is permitted, even if the purpose for such use is incompatible with the initial ones.

The first condition concerns the processing of data for archiving purposes in the public interest or for scientific, historical research or statistical purposes.[492] The term *statistical purposes*, although not further explained in the Regulation, can be seen as having a broad meaning, including not only the processing of data for the public interest but also the processing of data by business entities for commercial interests.[493] Within this context, profiling for statistical purposes can be considered to enable re-processing of data for further profiling without disregarding the purpose limitation principle.[494] This could also be regarded from the perspective that the Regulation authorises Member States to adopt measures to restrict the exercise of individuals' rights in relation to the re-processing of data for the aforementioned purposes.[495]

The second condition concerns the requirement of the data subject's consent. Article 6(4) states that where the purposes for further profiling are not compatible with the initial ones, such profiling will be legitimate only if the data subject has given his/her consent to such purposes or if the profiling is based on an EU or Member State law. It should be noted, however, that the consent as a legal justification is valid only if it is given 'for one or more specific purposes'.[496] In this way, the Regulation makes it more difficult for controllers to obtain consent for wide purposes and thus it further

[492] Article 5(1)(b) GDPR; See also Article 89 GDPR and Recital 156 GDPR which states that: '[t]he further processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is to be carried out when the controller has assessed the feasibility to fulfil those purposes by processing data which do not permit or no longer permit the identification of data subjects, (…)'.
[493] Mayer-Schonberger and Padova 2016 (n 75) 326.
[494] Mayer-Schonberger and Padova 2016 (n 75) 326.
[495] Recital 156 and Article 89(3) GDPR.
[496] Article 6(1)(a) GDPR.

limits the re-processing of personal data. [497]

4.5.3. Data Minimisation, Accuracy and Storage Limitation

The principle of data minimisation demands that the personal data should be adequate and not be excessive in relation to the purpose of the processing. In contrast to the DPD, the Regulation makes an attempt to strengthen this principle by requiring that the personal data are 'limited to what is necessary' for the purposes for which they are collected.[498] Thus, no more data than are necessary for the profiling should be processed.[499] Moreover, Recital 39 further states that personal data should be processed only if the purpose of the processing could not be reasonably fulfilled by other means. This implies that business entities should only process data for profiling if the purpose of the profiling cannot be reasonably fulfilled by other means.

Closely related to data minimisation are the accuracy and storage limitation principles. In relation to accuracy, the Regulation provides that every reasonable step should be taken to ensure that inaccurate personal data are rectified or deleted and that the individual must have the right to obtain, from the controller, the rectification of the inaccurate personal data concerning him/her.[500]

Regarding the storage limitation principle, the data should only be stored for the minimum period necessary. In other words, the data can only be held for the period necessary for the completion of the initial profiling for which they are collected. Recital 39 states that the period for which the data are stored should be 'limited to a strict minimum'. It does not, however, further clarify what the term *strict minimum* means or how it should be assessed.

[497] Mayer-Schonberger and Padova 2016 (n 75) 326.
[498] Article 5(1)(c) GDPR.
[499] Schermer 2013 (n 198) 147.
[500] Recital 39 GDPR.

In this way, it is up to each controller to determine the 'strict minimum' period for their processing activities. Similar to the purpose limitation principle, however, the Regulation permits the storage of data for longer periods than are necessary insofar as a new legal basis for further storage is justified (e.g. the individual has given his/her consent) (see section 4.6 on the legal basis of profiling) or the data will be processed solely for archiving purposes in the public interest or for scientific, historical research or statistical purposes (in accordance with Article 89(1) GDPR).[501] Obviously, the Regulation leaves room for further storage in relation to profiling for statistical purposes. For the effective application of the above three principles, the Regulation introduces the principle of 'data protection by design and by default' (for further analysis see section 4.8.5).

4.5.4. Integrity and Confidentiality

The new principle of integrity and confidentiality embraces the security of the personal data. Under this principle, business entities are obliged to adopt security measures to prevent unauthorised access to or use of the data or of the equipment (i.e. profiling technology) used for profiling.[502] To ensure, therefore, the integrity and confidentiality of the data, the Regulation obliges the controllers to adopt measures to ensure an appropriate level of security for the data and to perform data protection impact assessments (see sections 4.8.6 and 4.8.7 for further analysis).

4.5.5. Accountability

To enhance trust in the online environment and to fulfil the potentials of the Internal Market dimension, the GDPR demands more accountability for controllers. The accountability principle requires that controllers must adopt methods and practices 'to protect information in a manner more transparent to individuals and regulators'[503] and to be able to demonstrate these practices if asked to do so by the Data Protection

[501] Article 5(1)(e) GDPR.
[502] Recital 39 GDPR.
[503] Richard Thomas, 'Accountability – A Modern Approach to Regulating the 21st Century Data Environment' in Hielke Hijmans and Herke Kranenborg (eds), *Data Protection Anno 2014: How to Restore Trust? Peter Hustinx, European Data Protection Supervisor (2004-2014)* (Cambridge: Intersentia Publishing Ltd. 2014) 139.

Authorities (DPAs).[504]

In other words, business entities which engage in profiling are obliged to implement mechanisms in order to prove that their profiling activities are consistent with the data protection principles of the Regulation and, in particular, to ensure that they are effectively minimising the risks to the rights and freedoms of the individuals.

For this reason, the Regulation, unlike the DPD, establishes general obligations for controllers in order to ensure their accountability in the processing of personal data and their compliance with its provisions. In particular, Article 24(1) GDPR obliges the controllers to adopt policies and implement effective measures for ensuring and demonstrating compliance with the Regulation. These measures include the obligation for controllers to keep a record of all processing operations (Article 30 GDPR), to ensure the security of the processing (Article 32 GDPR), to perform data protection impact assessment (Article 35 GDPR), to cooperate with and consult the DPA (Articles 31 and 36 GDPR) as well as to designate a Data Protection Officer (Article 37 GDPR) and to introduce data protection certification mechanisms (seals and marks) (Article 42 GDPR).[505]

4.6. The Legal Basis for Profiling

Personal data can only be collected and processed if the processing is lawful. In order, therefore, to justify if a profiling activity is lawful, one of the following criteria specified in Article 6(1) have to apply: (a) the data subject has given his/her consent to the profiling for one or more specific purposes;[506] (b) profiling is necessary for the performance of a contract to which the data subject is party; (c) profiling is necessary for compliance with a legal obligation to which the controller is subject; (d) profiling is necessary in order to protect the vital interests of the data subject (e.g. to protect the individual's life); (e) profiling is necessary for the

[504] Thomas 2014 (n 503) 141; See also Article 29 Working Party, 'Opinion No. 3/2010 on the Principle of Accountability', adopted on 20th June 2007 (00062/10/EN, WP 173).
[505] The general obligation to notify the DPA under Articles 18(1) and 19 of the DPD is replaced by the obligation to keep records of all processing operations.
[506] Recital 32 GDPR.

performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; (f) profiling is necessary for the purposes of the legitimate interests pursued by a controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject (this does not apply to profiling activities by public authorities in order to perform their tasks).[507] In any case, profiling must be subject to suitable measures to safeguard the legitimate interests of the individual. In particular, the controller must enable human intervention and allow individuals to obtain further information regarding the profiling, as well as to express their point of view and to question the result of the profiling.[508]

Emphasis must be given to the requirement of consent. *Consent* is defined as 'any freely given, specific, informed and unambiguous indication of the data subject's wishes (…)'.[509] Therefore, in order for the consent to be legally justified, the controller must be able to prove that the individual has expressed his/her free, specific, informed and unambiguous agreement to the profiling.[510]

For the consent to be *free*[511] and *informed*[512], the individual must be properly and effectively informed, before the collection of his/her data, about the identity of the controller, the purposes for which his/her data are intended to be used and the potential implications of the profiling, in order to be able to freely and willingly give his/her consent.[513] In other words, consent must be the genuine and free choice of the

[507] Article 6(3) GDPR provides that the processing of data related to the points (c) and (e) should only take place if it is required by an EU law or the law of a Member State to which the controller is subject.
[508] Recital 71 GDPR.
[509] Article 4(11) GDPR.
[510] Articles 7(1) GDPR.
[511] 'Consent can only be valid if the data subject is able to exercise a real choice, and there is no risk of deception, intimidation, coercion or significant negative consequences if he/she does not consent. If the consequences of consenting undermine individuals' freedom of choice, consent would not be free' (Article 29 Working Party 'Opinion No. 15/2011 on the Definition on Consent', adopted on 13th July 2011 (01197/11/EN, WP 187) 12).
[512] '[C]onsent by the data subject (must be) based upon an appreciation and understanding of the facts and implications of an action. The individual concerned must be given, in a clear and understandable manner, accurate and full information of all relevant issues (…) such as the nature of the data processed, purposes of the processing, the recipients of possible transfers, and the rights of the data subject. This includes also an awareness of the consequences of not consenting to the processing in question' (Article 29 Working Party, 'Working Document on the Processing of Personal Data Relating to Health in Electronic Health Records (HER)', adopted on 15th February 2007 (00323/07/EN, WP 131) 8).
[513] Recital 42 GDPR; See also Maurizio Borghi, Federico Ferretti and Stavroula Karapapa, 'Online Data Processing Consent under EU Law: A Theoretical Framework and Empirical Evidence from the UK' (2013) International Journal of Law and Information Technology 21(2) 122.

individual (pre-ticked boxes are not admissible).[514] If the consent is subject to other conditions, and the individual is unable to refuse or withdraw his/her consent without suffering harm, such consent is not freely given (e.g. an individual is only allowed to use a service if he/she also consents to other processing activities, such as profiling for marketing or statistical purposes).[515] For this reason, the controller must enable the individual to give separate consent to different profiling activities.[516] For the consent to be *specific*,[517] the individual should be aware of the specific purpose of the profiling, at the moment of the collection of his/her data and before giving his/her consent. In this regard, Article 6 requires that consent must be given for one or more specific purposes in relation to the profiling. Therefore, consent given for general or unclear purposes (e.g. use of profiling for commercial purposes) cannot be regarded as binding. Finally, *unambiguous* consent requires a statement or a clear affirmative action on the part of the individual, which shows his/her acceptance of a particular profiling activity (e.g. written declaration or ticking a box when visiting a website).[518] There must be no doubt that the individual consented to that activity.[519] Therefore, silence, inactivity or the mere use of a service do not constitute unambiguous consent since they do not prove a clear indication of the individual's wishes.[520]

The Regulation provides that consent is not justified as a valid legal basis for profiling if 'there is a clear imbalance between the data subject and the controller'[521] (this is particularly the case where the controller is a public authority and the individual is unlikely to freely give his/her consent in all circumstances). Furthermore, where the individual is asked to give his/her consent in the context of a written declaration which also concerns other matters, the Regulation requires the controller to ensure that the individual is aware of the existence of those other

[514] Articles 6(1)(a) and 7 GDPR; See also Recital 42 and 43 GDPR.
[515] Recital 42 GDPR.
[516] Recital 43 GDPR.
[517] 'To be specific, consent must be intelligible: it should refer clearly and precisely to the scope and the consequences of the data processing. It cannot apply to an open-ended set of processing activities. This means in other words that the context in which consent applies is limited' (Article 29 Working Party Opinion No. 15/2011 (n 511) 17).
[518] Article 4(11) GDPR.
[519] Borghi, Ferretti and Karapapa 2013 (n513) 122.
[520] Christopher Kuner, Cetric Burton and Anna Pateraki, 'The Proposed EU Data Protection Regulation Two Years Later' (2014) Privacy & Security Law Report 2-3; See also Frederic Zuiderveen Borgesius, 'Behavioural Targeting: A European Legal Perspective' (2013) IEEE Security & Privacy 11(1) 84.
[521] Recital 43 GDPR.

matters, as well as of the extent to which consent is given.[522]

The addition of the right to withdraw consent and the conditions applicable to children's consent in relation to profiling purposes are of particular importance. Article 7(3) GDPR expressly provides for the individuals the right to withdraw their consent at any time. For this reason, controllers must offer to individuals as easily accessible and understandable methods by which to withdraw their consent as the methods provided to give the consent.[523]

However, the withdrawal of consent should not affect the lawfulness of profiling based on consent before its withdrawal. Additionally, the new Article 8 GDPR provides specific protection for children and sets out the conditions applicable to the child's consent in relation to profiling. The article provides that where the data subject is a child of at least 16 years old, profiling shall be considered as lawful provided that the child consents to the profiling (subject to Articles 6(1)(a) and 7 GDPR). Where the child is below the age of 16 years, his/her data can only be processed if the child's parent or custodian consents to the profiling.[524]

Another important element of Article 6 GDPR is that it limits the use of the controller's legitimate interest as a basis for lawful profiling. The article justifies the processing of personal data for profiling on the grounds of the controller's legitimate interest as long as the profiling does not override the rights and the interest of the data subjects (especially where the data subject is a child).[525] In such a case, the data subject should be informed about the legitimate interest of the controller and of his/her right to object to the profiling.[526]

One of the novelties of the Regulation is that it sets out the criteria under which

[522] Article 7(2) GDPR.
[523] The request for consent must be provided in an intelligible and easily accessible means, using clear and plain language and it should not contain unfair terms (Recital 42 and Article7(2) GDPR); See also Gehan Gunasekara, 'Paddling in Unison or Just Paddling? International Trends in Reforming Information Privacy Law' (2013) International Journal of Law and Information Technology 22(2) 27.
[524] The Regulation is empowered Member States to adopt rules for the processing of children's data for lower age provided that such age is not below 13 years (Article 8(1) GDPR).
[525] Recital 47 and Article 6(1)(f) GDPR.
[526] Recital 50 GDPR.

business entities can use legitimate interest as a legal basis to defend their profiling activities. According to Recital 47, consideration must be given to the reasonable expectations of the data subject based on his/her relationship with the controller.[527] A legitimate interest could exist if there is a relevant and appropriate relationship between the individual and the controller (i.e. where the individual is a client or in the service of the controller) and the individual can reasonably expect, at the time of the collection of his/her data, that profiling for that purpose may take place.[528] For example, an employee may have reasonable expectation that his/her employer has legitimate interest to further use his/her data for future promotions. In the absence of such reasonable expectation on the part of the employee, profiling is to be considered to override his/her fundamental rights and interests.[529]

In addition to the above, the Regulation also asserts that where profiling is strictly necessary to ensure network and information security (e.g. profiling is necessary to prevent unlawful and malicious actions or to stop 'denial of service' attacks or damages against the controller's systems), to prevent fraud or where it is used for direct marketing purposes, it is considered to be in the legitimate interest of the controller.[530] Likewise, further profiling (irrespective of its compatibility with the initial profiling) for the purpose of safeguarding the public interest (e.g. the controller is indicating possible criminal acts or threats to public security) can also be considered to be in the controller's legitimate interest as long as such profiling is compatible with the controller's legal, professional or other binding obligation of secrecy.[531]

Clearly, the Regulation, in contrast to the DPD, limits the use of the legitimate interest basis for the controllers. At the same time, however, it still provides a degree of flexibility for the controllers, either through the reasonableness test or by legalising a broad range of profiling activities (e.g. profiling for security, for fraud or

[527] Under the DPD, there is no uniform implementation of the legitimate interest element by the Member States. In Spain, for example, it is only provided for data collected from public sources while in Italy it only applies when the data protection authority has given its prior approval. (Richard Jones and Dalal Tahri, 'An Overview of EU Data Protection Rules on Use of Data Collected Online' (2011) Computer Law & Security Report 27 632).
[528] Recital 47 GDPR.
[529] Recital 47 GDPR.
[530] See respectively Recital 49 and 47 GDPR; See also Kuner 2012 (n 432) 9.
[531] Recital 50 GDPR.

for direct marketing purposes). The question which arises, therefore, is how the reasonableness and balancing tests will apply to determine, firstly, the reasonable expectations of the individuals and, secondly, the legitimate interests of the controllers *versus* the protection of the fundamental rights and values of the individuals.

In the context of profiling, the CJEC, in the case of *Google Spain*, made an attempt to further limit the use of the legitimate interest basis by ruling that the processing of personal data carried out by the operator of a search engine is liable to significantly affect the fundamental rights to privacy and to the protection of personal data of the individual concerned, since that processing enables any internet user to obtain information relating to that individual's personal aspects and, therefore, allows the establishment of a more or less detailed profile of the individual.[532] From this perspective, the Court also ruled that such processing of personal data cannot be justified merely by the economic interest – legitimate interest – of the operator of the search engine.[533]

4.7. Profiling Based on Special Categories of Data

One of the key elements of the Regulation is that it prohibits profiling that is based on special categories of personal data – sensitive data – or on data relating to children. In particular, the Regulation prohibits profiling based on sensitive data 'revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union memberships, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation'[534] (Article 9 GDPR expands its scope to genetic and biometric data and, in this respect, it differs from the DPD). If, for example, an employer categorises its potential employees into profiles based on their sex life (e.g. 'heterosexual' and 'homosexual' applicants) or if a retailer categorises its customers into profiles based on their race ('black' and

[532] *Google Spain* Case (n 478) para. 80.
[533] *Google Spain* Case (478) para. 81.
[534] Article 9(1) GDPR.

'white' customers), such profiling would be unlawful and prohibited.

Interestingly, Recital 51 considers the processing of photographs by stating that such processing is covered by the definition of biometric data[535] and that it should not systematically be considered as processing of sensitive data unless the photographs are processed through specific technical means which allow the identification or the authentication of the individual. In other words, photographs constitute sensitive data as long as they are processed through the use of biometric systems (e.g. face recognition technology) for the purpose of identifying or authenticating a person (e.g. fingerprints, hand geometry or facial images). Obviously, the wording of Recital 51 excludes from the scope of the Regulation photographs merely taken either by the individual him/herself or by another person.

Nevertheless, to the extent that profiling involves the processing of sensitive data, Article 9(2) GDPR requires that the individual must give his/her explicit consent for the profiling to be lawful. In the absence of the individual's explicit consent, Article 9(2) GDPR provides exceptions to the general prohibition of Article 9(1) GDPR.[536]

---

[535] 'biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data' (Article 4(14) GDPR).

[536] Article 9(2) GDPR provides that:
'Paragraph 1 shall not apply if one of the following applies: (a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject; (b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject; (c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent; (d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects; (e) processing relates to personal data which are manifestly made public by the data subject; (f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity; (g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject; (h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3; (i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy; (j) processing is

Accordingly, the Regulation, like the Directive, does not provide an explicit prohibition of the processing of sensitive data. While, on the one hand, the Regulation renders illegal the profiling activities based on sensitive data, on the other hand, it qualifies a number of conditions under which such profiling can be permissible.

4.8. Specific Rules for Profiling

One of the important elements of the Regulation is that it provides specific rules for profiling. As previously mentioned, in order to achieve the goal of the fairness and transparency principles, the Regulation provides the individuals with a set of data protection rights that enable them to have access to and to obtain control over their personal data. In addition, based on the principle of accountability, the Regulation establishes general obligations for the controllers and processors in order to ensure their responsibility to the profiling process and their compliance with its rules. The next section, therefore, examines the rights and obligations conferred under the Regulation.

4.8.1. The Right to be Informed

The first right granted to individuals is introduced under Articles 13 and 14 GDPR and provides that the data subjects must be informed about the collection and processing of their personal data. In particular, it obliges the controller to provide to individuals the list of information set out in Article 13 GDPR,[537] as well as

necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.'

[537] The controller shall, at the time when personal data are obtained, provide the data subject with all of the following information: '(a) the identity and the contact details of the controller and, where applicable, of the controller's representative; (b) the contact details of the data protection officer, where applicable; (c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing; (d) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party; (e) the recipients or categories of recipients of the personal data, if any; (f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

information regarding the existence of automated decision-making, including profiling, the logic involved in the profiling and the significance and envisaged consequences of such profiling to them (in comparison with Article 10 DPD, the list of information provided under Article 13 GDPR has been extended and improved).[538] All of this information must be given to the individual at the time of the collection of his/her personal data.[539]

Where the data are not collected from the data subject but from another source, the controller is still obliged to provide to the data subject a list of information similar to the list set out in Article 13 GDPR, including the existence of profiling and its envisaged consequences to him/her.[540] The information must be given within a reasonable amount of time after the collection and at the latest within one month, depending on the circumstances of the case.[541]

However, Article 14(5) GDPR additionally provides that the obligation of controllers to provide this information does not apply either where the individual already has the information in his/her possession, or where the communication of the information is impossible or it involves a disproportionate effort, or where the obtaining or disclosure of the individual's data is expressly laid down by the law, or where the personal data must remain confidential subject to professional secrecy.[542] As with the DPD, there is no further clarification of what constitutes *disproportionate effort* under the Regulation. The only reference is made under Recital 62 which states that information to be provided for data processing for historical, statistical or scientific research purposes may need a disproportionate effort on the part of the controller to communicate the information because of the number of data subjects involved or the age of the data.

[538] Article 13(2)(f) GDPR.
[539] It should be noted that, under the DPD there is no provision establishing the time when the information has to be given to the data subject. The Article 29 Working Party on its document on Blacklist has stated that 'one way of avoiding errors and problems would be to lay down a reasonable period between notification of the data subject and the actual entering of the information on the joint file, and this procedure could also apply to files on breaches of monetary obligations' (Article 29 Working Party, 'Document on the Blacklist', adopted on 3th October 2002 (11118/02/EN, WP 65) 8).
[540] Article 14(2)(g) GDPR.
[541] Recital 61 and Article 14(3) GDPR.
[542] Recital 62 and Article 14(5) GDPR.

4.8.2. The Right of Access

Along the same lines, the right for individuals to access their data explicitly refers to profiling.[543] In this way, the Regulation enables individuals to be aware of, and ensure, the lawfulness of the profiling and the accuracy of their data.[544] This right is provided also by Article 12 DPD and refers to the right of individuals to obtain knowledge of the logic involved in any automated processing of their data. However, in the new technological environment it has been proven to be difficult, in practice, for individuals to exercise this right, especially with the vast amount of data collected and stored in the databases.

Thus, the Regulation aims to reinforce the individuals' right of access to their data by giving them the right to obtain, on request, confirmation of the existence of automated decision-making, including profiling, information regarding the logic involved in the profiling and its significance and envisaged consequences to them. In this respect, individuals will be aware of any false negative or false positive evaluations and judgements of their current or future behaviour and conditions and thus will be allowed to object to the application of the profiles.[545]

Furthermore, in the case where the personal data is transferred to a third country or to an international organisation, the Regulation grants to the individuals the right to be informed of the safeguards taken in relation to such transfers.

4.8.3. The Right to Object

Another important right is the right to object to profiling. Article 21 GDPR provides individuals the right to object to a profiling activity, even when such activity is lawful. This right is based on Article 14 DPD and provides that where the profiling is lawfully made, subject to Article 6 GDPR, for the purpose of public interest or the

[543] Article 15 GDPR.
[544] See also Recital 63 GDPR.
[545] Schreur et al. 2008 (n 482) 253.

exercise of official authority, or the legitimate interests of a controller,[546] the individual should have the right to object to the profiling unless the controller proves that there are 'compelling legitimate grounds'[547] for this profiling which may override the interests or fundamental rights and freedoms of the individual. In other words, the burden of proof resides with the controllers to prove the existence of 'compelling legitimate grounds' for the profiling.

The right to object also applies to profiling for the purpose of direct marketing. Thus, individuals should be able, at any time and free of charge, to object to direct marketing which includes profiling.[548] In this case, the controller must stop the profiling. The right must be offered clearly, explicitly and must be distinguishable from other information.[549] Furthermore, the controller should also provide automated means using technical specifications in order to entitle the individual to object electronically, in particular where the processing of personal data has taken place by electronic means.

4.8.4. The Right not to be Subject to an Automated Decision, including Profiling

Of particular importance is the right not to be subject to decision-making based on the automated processing of personal data, including profiling. In particular, Article 22(1) GDPR provides that:

> 'The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.'

In order, therefore, for the right of Article 22(1) GDPR to apply, the following

[546] Article 6(1)(e) and (f) GDPR.
[547] Recital 69 and Article 21(1) GDPR.
[548] Article 21(2) GDPR.
[549] Recital 70 and Article 21(4) GDPR.

elements must be satisfied: (a) a decision must be made; (b) the decision must be based solely on profiling; and (c) the decision concerned must produce legal effects or significantly affect the data subject for whom the decision is made. If any one of the aforementioned elements is not fulfilled, the decision is not qualified as an automated decision based on profiling and thus Article 22 GDPR does not apply.

In connection with the first element, Recital 71 states that the decision could be a measure evaluating an individual's personal aspects. As already stated, a measure involves any course of action that is taken to reach a particular outcome and that action could be a decision (see section 4.4.1).[550] In addition, as it is seen above, profiling constitutes any form of automated processing of personal data evaluating an individual's personal aspects, in particular to analyse or predict aspects concerning his/her performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.[551] This means, therefore, that a fourth element of Article 22(1) GDPR is that the decision must involve the intention of the controller to evaluate, analyse or predict personal aspects relating to individuals. For example, a university processing a student's data with the intention of assessing his/her educational progress and his/her probability of graduating.

The second element of Article 22(1) GDPR requires that the decision – measure – must be based solely on profiling. This means that not only the collection and processing of data but also the outcome of the decision-making process must be executed by a machine without the involvement of human intervention.[552] However, what this element stipulates is not the absence of human involvement in the entire profiling process but rather it indicates that the decision must be based solely on the results produced by the profiling.[553]

---

[550] Vermeulen 2013 (n 123) 8.
[551] Recital 71 and Article 4(4) GDPR.
[552] Recital 71 GDPR.
[553] The Commission in its amended proposal for the DPD explained that 'what is prohibited is the strict application by the user of the results produced by the system. Data processing may provide an aid to decision-making, but it cannot be the end of the matter; human judgement must have its place' (COM(92) 422 final – SYN 287, 15.10.1992, p26 <http://aei.pitt.edu/10375/1/10375.pdf> (accessed 1 May 2016)); See also Bygrave 2001b (n 442) 20; Meike Kamp, Barbara Korffer and Martin Meints, 'Profiling of Customers and Consumers – Customer Loyalty Programmes and Scoring Practices' in Mireiller Hildebrandt and Serge Gutwirth (eds), *Profiling the European Citizen: Cross-Disciplinary Perspectives* (Springer Science+Business Media 2008) 210.

In his analysis of Article 15 DPD, Lee Bygrave explains that a decision is considered to be *solely* automated if 'a person fails to *actively* exercise any *real* influence on the outcome of a particular decision-making process'.[554] He further explains that such a situation exists where a decision results from the automated processing of data and is ascribed to an individual without being actively assessed either by the individual or the controller.[555]

For example, where the decision of a bank to reject a loan applicant is based entirely on his/her credit scoring results, or the rejection of a job applicant is based entirely on the results of his/her computer-based personality test, without the re-evaluation of the results by a human (e.g. the bank officer or the employer), the decision can be said to originate *solely* from the automated processing of data – profiling. Both the credit scoring and the personality test are the results of automated evaluation, analysis or prediction of the individuals' personal aspects (as produced by the profiling process). Neither the bank nor the employer re-assess or re-consider the results along with the real conditions of the applicant before making their decision. In the case of the job applicant, for example, the employer could re-assess the results of the personality test by also taking into account other factors in the making of his/her decision, such as the applicant's personality, the answers he/she gave in the personal interview or his/her knowledge on a particular subject. Thus, the result of the personality test constitutes the only determining factor for the employer to make his/her decision (to reject the applicant) so that the whole process can be seen to take place automatically by a machine and not by the employer.

It follows, therefore, that the second element of Article 22(1) GDPR presupposes that the decision is the result of the automated evaluation, analysis or prediction of personal aspects of the individual concerned without the involvement of either the individual or the controller to re-evaluate the results. In short, the application of the profiles is based solely on the knowledge inferred from them. In cases where the decision does not have legal effects or it does not similarly significantly affect the

[554] Bygrave 2001b (n 442) 20.
[555] Bygrave 2001b, (n 442) 20.

individual, Article 22(1) GDPR does not apply. Neither the DPD nor the GDPR elaborate further on the terms *legal effects* and *significantly affects*. Recital 71 refers, by a way of example, to the situations of automatic refusal of an online credit application or e-recruiting practices (without any human intervention).

In derogation to the right provided under Article 22(1), a decision based on automated processing, including profiling, can only be allowed if it is lawful. Article 22(2) GDPR, therefore, provides the conditions for the legal justification of such decisions. It requires that a decision based on profiling can only be allowed if one of the following criteria applies: (a) the decision is necessary for entering into, or performance of, a contract between the data subject and a controller; (b) the decision is authorised by an EU or Member State law (e.g. for fraud and tax-evasion monitoring and prevention purposes, as well as for ensuring the security and reliability of the controller's service) to which the controller is subject; (c) when the data subject has given his/her explicit consent to the decision subject to Article 7 GDPR.[556] In addition, Recital 71 expressly states that such a decision should not concern a child. Although these criteria are similar to those under Article 15 DPD, Article 22 GDPR imposes consent as an additional requirement in order for such a decision to be permissible. In any case, the controller must implement suitable measures to safeguard the rights and freedoms and the legitimate interests of the individual and provide him/her with the right to obtain human intervention, to express his/her view, to receive explanation of the decision and to contest the decision.[557] Additionally, the Regulation is also empowered by the European Data Protection Board (the 'Board), which succeeds the Article 29 Working Party, to specify the criteria and conditions under which decisions based on profiling will be permitted in order to enforce the controllers to adopt better and uniform practices.[558] Finally, one of the key additions of Article 22 GDPR is that it prohibits automated decision-makings that are based on special categories of personal data – sensitive data – referred to in Article 9 GDPR, and on data relating to children (see section 4.7 which examines profiling based on special categories of personal data).[559] If, for

[556] Recital 71 and Article 22(2) GDPR.
[557] Recital 71 and Article 22(3) GDPR.
[558] Article 70(1)(f) GDPR.
[559] Recital 71 and Article 22(4) GDPR.

example, a retailer profiled its customers based on their race ('black' and 'white' customers) and decided to offer different prices to 'white' customers, such a profiling-based decision would be unlawful.

However, to the extent that a decision is to be made based on the individual's sensitive data, Article 22(4) GDPR requires that either the individual gives his/her explicit consent to the decision or that the decision is considered to be necessary for reasons of substantial public interest, on the basis of Union or Member State law. In such cases, the controller, in order to ensure the fairness and transparency of the profiling and to prevent discriminatory effects on individuals (based on their sensitive data), is obliged to use appropriate mathematical or statistical procedures for the profiling and to implement technical and organisational measures to ensure that inaccurate personal data are corrected and that the risk of errors is minimised.[560]

Apparently, Article 22 GDPR develops the basic elements of Article 15 DPD, while making an attempt to strengthen the protection of individuals by regulating, specifically, decision-makings based on profiling.[561] However, similar to Article 15 DPD, the problem with Article 22(1) GDPR is that, in the end, its application depends on the action of the individual – 'data subject shall have the right not to be subject to a decision'. This means that it does not provide a direct prohibition but it gives to the individuals the opportunity to exercise the right if they wish to do so.[562] As stated by Bygrave, '[t]his would leave the actual exercise of the right to the discretion of each person and allow, in effect, the targeted decision making to occur in the absence of the right being exercised (…)'.[563] In this meaning, the right provided under Article 22(1) GDPR is equivalent to a right to object to a profile-based decision, provided that the individual chooses to exercise it.

[560] Recital 71 GDPR.
[561] The article is also influence by Article 3 of the Council Recommendation CM/Rec(2010)13 (n 416).
[562] Bygrave 2001b (n 442) 18.
[563] Bygrave 2001b (n 442) 18.

4.8.5. Data Protection by Design and by Default

For the effective application of data minimisation, accuracy and storage limitation principles, the Regulation introduces the principle of 'data protection by design and by default' which mandates the controllers to adopt state-of-the-art technology to ensure that, by default, only the minimum data necessary for each particular purpose are processed and that such data are pseudonymised as soon as possible.[564] The purpose of this principle is to ensure that personal data are not made accessible, by default, to the public.[565] There are, for example, online social networks which, by default, do not protect privacy unless the user manually chooses that option (e.g. Facebook's default settings allow a user's profile to be available to the public unless the user chooses otherwise). The meaning of the term *by default* is not further explained in the Regulation, but it is presumed to refer to privacy-friendly technologies (e.g. technologies which enable, by default, privacy-friendly settings such as the blocking of third-party cookies or the automatic selection of buttons like 'Do Not Track' or 'Protect My Privacy').[566]

4.8.6. Security of the Data

In order to reinforce the security of profiling and to prevent data breaches, the Regulation requires the use of technical and organisational measures to protect the privacy of the data (e.g. privacy-friendly default settings). In particular, Article 32 GDPR regulates the security of personal data by obliging the controllers and the processors to adopt measures to ensure an appropriate level of security for the data, taking into account the state of the art, the cost of their implementation and the nature, scope, context and purposes of profiling, as well as the potential risk to the rights and freedoms of the individual (the difference with Article 17(1) DPD is that Article 32 GDPR extends its scope also to processors). Such measures include: (a) the pseudonymisation and encryption of personal data; (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of profiling

[564] Recital 78 and Article 25 GDPR.
[565] Kuner, Burton and Pateraki 2014 (n 520) 2–3.
[566] Kuner 2012 (n 432) 13.

technologies; (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the profiling.[567]

4.8.7. Data Protection Impact Assessment

As a result of the accountability principle, business entities are required to implement mechanisms in order to ensure the adequate and effective protection of individuals' personal data. In particular, Article 35 GDPR obliges the controllers to carry out a risk analysis of the potential impact of their profiling activities upon the rights and freedoms of individuals.[568] Thus, every time a profiling takes place, a business entity is obliged to assess whether profiling is likely to pose high risks to the rights and freedoms of individuals.

The impact is to be assessed according to the nature, the scope, the context and the purpose of the profiling (e.g. the broader the scope of a profiling activity, the greater the impact on individuals might be).[569] For example, if a business entity intends to process biometric data in a large-scale system, it must evaluate the possible risks to the individuals concerned, inform the individuals of such risks and adopt measures to reduce the risks.

The controller must seek the view of the individual and consider it in conjunction with the security of the profiling and the protection of commercial and public interests (Article 35(9) GDPR) and must communicate the impact assessment to the DPA, prior to the processing of personal data, in order to ensure compliance of the profiling with the Regulation and to assess the potential risks for the protection of

[567] Article 32(1) GDPR.
[568] Article 35(3) GDPR provides a list of processing operations which are likely to present high risks to individuals. These operations include: '(a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person; (b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or (c) a systematic monitoring of a publicly accessible areas on a large scale'.
[569] Gunasekara 2013 (n 523) 23.

individuals (Article 36 GDPR).[570] In addition, the Regulation empowers the DPA to publish a list of the types of processing activities which require a data protection impact assessment and a list of those processing activities which do not require a data protection impact assessment.[571]

4.8.8. Data Breach Notification

In the case of a data breach that is likely to result in a high risk to the rights and freedoms of individuals, a general obligation is introduced for controllers to notify the breach to both DPAs and to the individuals concerned, without undue delay (the processors are also obliged to notify the controller immediately after establishing that a personal data breach has occurred).[572] If it is unlikely to affect the rights and freedoms of individuals, notification does not need to be communicated either to the DPA or to the individual.[573] Additionally, the controller is not obliged to communicate the breach to the individual if he/she has implemented all the appropriate technological and organisational measures for the protection of the individual's data, he/she has taken additional measures to minimise the possibility of the risk, or the communication of the breach will involve disproportionate effort (in such a case the controller should use another way to effectively inform the individual).[574]

The notification must describe the nature of the personal data breach, its consequences, the measures taken by the controller to address it and the contact details of the Data Protection Officer (where more information can be obtained), as well as recommendations to the individuals to mitigate the potential effects of the breach.[575] In the case of notification to DPAs, such notification must be given, where

[570] For similar processing operations that present similar high risks for individuals, the controller can carry out a single impact assessment covering all the similar operations in order to reduce the cost (Article 35(1) GDPR).
[571] Article 35(4)–(5) GDPR.
[572] Articles 33 and 34 GDPR.
[573] According to Recital 85 GDPR, a breach is likely to involve a high risk to the rights and freedoms of individual if it results in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned.
[574] Article 34(3) GDPR.
[575] Article 33(3) and 34(3) GDPR.

feasible, within 72 hours after the controller becomes aware of the breach, unless he/she provides a justified reason for the delay.[576]

4.8.9. Data Protection Officer

One of the key elements of the Regulation is the requirement to create a Data Protection Officer (DPO) position. Article 37 GDPR provides the mandatory appointment of a DPO for the public sector and, for the private sector, where the core activity of the controller or the processor consists of either processing operations which, by virtue of their nature, their scope and purposes require regular and systematic monitoring of individuals, or it consists of the processing, on a large scale, of sensitive data and personal data relating to criminal convictions and offences referred to in Article 10 GDPR.

In support of this new requirement, the Regulation incorporates, under Articles 37 to 39 GDPR, detailed rules for the appointment, the position and the duties of the DPOs, including their qualification requirements (e.g. expert knowledge of data protection law), the period of their appointment (e.g. for at least two years) and the power to perform their duties independently. It should be added that in the case of a group of business entities with establishments in more than one Member State the group could appoint a single DPO.[577]

The appointment of DPOs is expected to bring positive results to the protection of individuals, as well as to the EU business industry, since it will enable controllers to comply more effectively with their obligations under the Regulation[578] and it will create new positions for employment, education and training in the area of data protection. This, of course, implies more costs (e.g. salary, training, equipment etc.) for those business entities which fulfil the criteria of Article 37 GDPR.

Following the above, it should now be asked whether the Regulation does indeed

[576] Recital 85 and Article 33(1) GDPR.
[577] Article 37(2) GDPR.
[578] See Article 39 GDPR on the tasks of DPO.

fulfil its objectives of providing both a high level of protection for the fundamental rights and freedoms of individuals (both inside and outside of the EU) while, at the same time, allowing the free movement of personal data in the Internal Market. Furthermore, it should also be asked whether the Regulation has strengthened the protection of individuals' rights, in relation to profiling, beyond the protection provided under the DPD.

Generally, the answer to both of the above questions seems to be positive, at least theoretically. As a transparency mechanism, the new data protection legislation accepts the legitimate interest of controllers to do business and thus to use personal data for their profiling activities. Yet, it accepts the right of individuals to data protection against profiling. It empowers, therefore, individuals' positions to exercise control over their personal data while at the same time it enables the controllers to use profiling for their commercial interests.

However, although a law may serve its purposes, it does not necessarily protect the individuals adequately and effectively. Therefore, the issue that still remains is whether the protection provided under the Regulation is adequate and effective to secure the fundamental rights and values of the individuals, notably their rights to privacy and data protection, within the context of profiling. As previously mentioned (in section 4.4.1), the actual effectiveness of the new data protection legislation can only be determined by examining the true extent to which the provisions of the Regulation achieve its respective objectives in relation to profiling. In order, therefore, to assess the effectiveness of the Regulation to adequately protect individuals, it is necessary to examine the full extent to which the Regulation applies, in practice, as well as its actual level of protection of the individuals with regards to profiling.

Chapter 5

Balancing Profiling and Human Rights Protection

5.1. Introduction

The foregoing chapter attempted to show how the EU data protection legislation deals with profiling and its challenges to the fundamental rights and values of individuals, notably to the rights to privacy and data protection. In doing so, the chapter examined how the GDPR regulates profiling. As it showed, the GDPR brings with it some degree of innovation and some degree of consistency, in the sense that the text of the Regulation relies on the key provisions of the DPD but also adds new ideas and principles. As a Regulation, the new data protection legislation aims to eliminate the legal divergence between EU Member States by providing a greater degree of uniformity for data protection in Europe. Such uniformity entails that the level of data protection and the application of the provisions of the Regulation should be the same in all EU Member States. The scope of the application of the Regulation is broadened to cover processing activities concerning European data subjects, not only by EU but also by non-EU based controllers and processors. In this way, the Regulation increases the level of data protection for individuals who are subject to profiling activities outside the EU.

One of the significant changes of the GDPR is that it sets out specific rules governing profiling. In this way, the GDPR affirms that the processing of personal data for profiling is subject to the scope of the new data protection legislation. The Regulation aims to strengthen the protection of individuals in relation to profiling by empowering their position and their ability to exercise control over their personal data, whereas it imposes on controllers more obligations to ensure their accountability and transparency in the profiling process. For this reason, it regulates not only the decision-makings resulting from the application of the profiles but also the creation of profiles. In particular, the GDPR provides an explicit definition of profiling which incorporates both the creation and application of profiles. In

addition, profiling is subject to the data protection principles of the Regulation and the provisions regulating the lawfulness of the processing of data.[579] This means that profiling must be fair, lawful and transparent.

Highly significant in the Regulation is the requirement of lawfulness. For the profiling to be lawful, the GDPR provides that there must be a legal basis to justify it. Just like the DPD, the GDPR remains consistent with the notion of consent: the processing of personal data cannot be done without the consent of the data subject. Consent is the main condition for lawful profiling and lawful decision-makings based on profiling. It is the foundational element of the EU data protection legislation and ensures the fair, lawful and transparent processing of individuals' personal data. For this reason, the GDPR strengthens the requirement of consent by demanding that consent must be also the unambiguous indication of the individual and that it must be given for specific profiling purposes. Moreover, the Regulation requires that individuals must consent not only to the creation of a profile but also to its application.

In light of these changes, therefore, one might argue that the new data protection legislation moves towards greater protection for individuals in relation to profiling and greater responsibility for controllers, that goes beyond the protection and the responsibility provided under the DPD, while at the same time allows controllers to process personal data for their profiling activities. However, in a profiling-based environment, with personal data being collected and analysed at an unprecedented level, the effectiveness of the GDPR to ensure fair, lawful and transparent profiling activities is questionable. Yet, it is questionable whether consent can fulfil the demands of a profiling-based environment, by effectively and adequately protecting individuals' autonomy and their right to self-determination, and thus maintaining their privacy and their right to data protection.

The purpose of the present chapter is, therefore, to examine whether, in practice, the protection provided under the GDPR is adequate and effective to secure the

[579] Articles 5–6 GDPR.

fundamental rights and values of the individuals, notably their rights to privacy and data protection, within the context of profiling. For this reason, the chapter will bring together the findings of the previous chapters in an attempt to answer the following questions: Does the GDPR effectively minimise the asymmetries of knowledge and the unbalanced distribution of powers between the controllers and the individual subjects, resulting from the use of profiling? Does the GDPR protect individuals from group profiles? Is consent (as a legal requirement) an effective mechanism for individuals to preserve their autonomy and their right to self-determination? To what extent can the individual's control over his/her personal data be achieved in a profiling-based environment?

The chapter is organised as follows: in section 5.2, the chapter examines the possible problems that may arise in relation to the applicability of the GDPR in the context of profiling. The analysis is extended by the detailed analysis of the problems arising in relation to the use of group profiling (section 5.2.2). The next section discusses the protection offered to individuals against profiling and the problems that may arise when the GDPR applies (section 5.3). In particular, the section examines whether the applicability of data protection principles is effective in view of profiling (section 5.3.1). Section 5.4 deals with the legal basis of consent. In particular, the section examines whether consent under the GDPR is a real choice or a pseudo-right.

5.2. The Problem with the Applicability of GDPR

One of the most disputed issues in the GDPR is the scope of its application. The Regulation applies only to the processing of personal data.[580] The processing of data that are not qualified as personal is excluded from the scope of the Regulation. In addition, Article 4(4) GDPR defines profiling as any form of automatic processing of personal data for the purpose of evaluating, analysing or predicting certain personal aspects relating to a natural person. Therefore, for the profiling to be subject to the

[580] Article 2(1) GDPR.

scope of the Regulation there must be processing of personal data. That is, the data of an identified or an identifiable natural person.[581]

In Chapter 4, identifiability was discussed in view of the opinion of the Article 29 Working Party on the concept of personal data.[582] According to the Article 29 Working Party, the main criterion for identifiability is whether the individual can possibly be singled out, directly or indirectly, within a group of people.[583] Therefore, an identifiable individual is one who can be identified, directly or indirectly, from data based on certain identifiers.[584] To determine whether an individual is identifiable or not, it is necessary to consider all the means which are reasonably likely to be used either by the controller or by any other person to identify the said individual (it is not relevant who can identify the individual).[585] In other words, as long as the data can reasonably be linked to an identifiable individual, they are considered to be personal data and thus within the scope of the GDPR. In the absence of a reasonable possibility of linking the data to an identifiable individual, the data are not personal and are excluded from the scope of the Regulation.[586] This exclusion also includes cases where personal data are rendered anonymous in such a way that the individual is no longer identifiable.[587]

With regard to profiling, however, such exclusions are questionable since (as it will be seen below) profiling may apply to an individual even if that individual is not identifiable within the meaning of the Regulation.[588]

5.2.1. Identifiability and Profiling

Personal data is defined in Article 4(1) GDPR as any information relating to an identified or identifiable natural person (data subject). According to Lee Bygrave,

[581] Article 4(1) GDPR.
[582] See section 4.4.2.1 in Ch 4.
[583] Article 29 Working Party, Opinion No. 4/2007 (n 425) 12.
[584] See p.139 in Ch 4.
[585] Recital 26 GDPR.
[586] Schreur et al. 2008 (n 482) 243, 246–247.
[587] Recital 26 GDPR.
[588] Schreur et al. 2008 (n 482) 243, 246–247; See also Gutwirth and Hildebrandt (2010) (n 189) 6.

this definition incorporates two elements: (a) the data must facilitate the identification of the individual (identifiability elements) and (b) the data must relate to or concern that individual (data–person relation elements).[589] If either of the two elements is not fulfilled, the data are not personal and the GDPR is not applicable. The question, therefore, is whether the data being processed for profiling satisfy these two elements.

The first case to be examined is that of individual or personalised profiling. As explained in Chapter 1, personalised profiling concerns a set of correlated data (profile) that identifies and represents one particular individual.[590] The profile is based on the characteristics and behaviour of that particular individual (e.g. his/her shopping habits or product preferences). Applying, therefore, the concept of personal data, personalised profiling seems to satisfy both elements: the profile identifies one particular individual (identifiability element) and relates to the data about that individual (data–person relation element). However, identification in personalised profiling does not necessarily mean that the individual is identifiable within the meaning of the GDPR.[591] In the case of biometric behavioural profiling, for instance, the use of facial recognition technologies can collect real-time (anonymous) information about an audience's emotional reactions towards a product, a speech or a campaign and create personalised, emotional profiles without linking the profiles to identifiable individuals.[592] In this case, although the profile may continuously identify the individual as the same person over a period of time, the individual is not identified by his/her name but by the serial number assigned to him/her. In this context, the profile is not considered to be the personal data of an identifiable

[589] Bygrave 2002 (n 263) 42.
[590] See section 1.7.1 in Ch 1.
[591] Schreurs et al. 2005, FIDIS Deliverable D7.3 (n 55).
[592] A good example is the Microsoft's 'Realtime Crowd Insights' software (an Application Programming Interface (API) that connects web applications to Microsoft cloud computing services) which can read the facial expressions of the crowds at political campaigns and create personalised emotional profiles for each participant. With the use of camera, the software collects the face image of each person in the crowd and sends them to Microsoft servers. Microsoft then analyse the images and return with a profile for each person. Each profile includes an assigned serial number (e.g. 'b2ff') and several pieces of information about the person such as an estimation of his/her age, gender, ethnicity, clothing style, time of attention and any emotions detect (e.g. anger, fear, happiness etc.). The persons are not identified by their names but only by their serial numbers (Alex Emmons, 'Microsoft Pitches Technology That Can Read Facial Expressions at Political Rallies' (2016) <https://theintercept.com/2016/08/04/microsoft-pitches-technology-that-can-read-facial-expressions-at-political-rallies/> (accessed 18 August 2016)).

individual. It follows, therefore, that although personalised profiling normally satisfies both elements of personal data, there may be cases where the profile contains no personal or anonymous data and so cannot facilitate the identification of the individual and thus the GDPR is not applicable.[593] In such a case, the GDPR is not applicable and the individual has no rights upon his/her data.

The second case to be examined is that of group profiling. Identification in group profiles does not imply the knowledge of the actual identity of the individual. The profile identifies and represents a group (community or category) of individuals sharing one or more common characteristics.[594] The profile is not interested in the characteristics of a particular individual. It reveals knowledge about the habits, preferences, behaviour and lifestyle of a certain group of people (e.g. reading habits of lawyers or shopping preferences of Spanish customers).[595] Thus, the purpose of the profile is to identify the individual as a member of a particular group, rather than to distinguish him/her from the other members of the group (as a specific individual). In other words, identification in group profiling refers to the knowledge that the individual is a member of a particular group rather than the knowledge of his/her actual identity. As such, for group profiling it is not necessary for the individual to be identifiable in the sense of the GDPR. The profile applies to those individuals (identifiable or not) whose data match the characteristics of the profile.[596]

This means that the data used for the profile may not be the personal data of the individual to whom the profile is applied. As a result, there may be cases where group profiles do not satisfy either the element of identifiability nor the element of data–person relationship (that is the case for non-distributive group profiles).

[593] Schreurs et al. 2005, FIDIS Deliverable D7.3 (n 55).
[594] See section 1.7.1 in Ch 4.
[595] Hildebrandt 2009b (n 184) 151; See also Schermer 2013 (198) 145.
[596] In group profiling, a person may be identifiable in the case of distributive group profile where the profile applies to the group as a whole but also to each single member of the group in the form of individual profile. For instance, if all the individuals in a certain group are London citizens having a specific type of sun allergy, then if an individual is known to be a member of that group (he/she is a London citizen having that specific type of sun allergy), he/she can easily be distinguished from the group.

So viewed, the concept of personal data limits the applicability of the GDPR in relation to profiling practices:[597] firstly, because many profiles (especially group profiles) can be created without the use of personal data but rather with the use of non-personal data and, in particular, of anonymous personal data to which the GDPR does not apply;[598] and secondly, because group profiles do not necessarily apply to an identifiable individual.[599] In this regard, two issues are at stake in relation to the protection of individuals: the application of group profiles and the use of anonymous data.

5.2.2. The Problem with Group Profiling

The first issue to be considered is the protection of individuals against group profiles. As it is explained above, a group profile does not demand the identifiability of individuals in the meaning of the GDPR. Identification, in this case, refers to the knowledge that the individual is a member of a particular group rather than to the knowledge of his/her actual identity. For this reason, a group profile may either apply to an identifiable individual or to a non-identifiable individual. Obviously, from a legal perspective, this situation creates problems.

If the group profile applies to an identifiable individual (i.e. the profile is based on personal data), the GDPR applies which means that the profiling is subject to the rules of the Regulation and that the rights of the individual and the obligations of the controller with regard to the data are activated. If, however, the group profile applies to a non-identifiable individual (i.e. the profile is based on non-personal or anonymous data), the GDPR does not apply and the individual has no rights and the controller no obligations with regard to the data. The most problematic type of group profiling is that of non-distributive group profiles.

[597] Schreur et al. 2008 (n 482) 243, 246–247; See also Gutwirth and Hildebrandt (2010) (n 189) 6.
[598] Schreurs et al. 2005, FIDIS Deliverable D7.3 (n 55).
[599] Hildebrandt, Gutwirth and Hert 2005, FIDIS Deliverable D7.4 (n 284) 45; See also Hildebrandt 2009b (n 184) 250.

As explained in Chapter 1, a non-distributive group profile is a group profile where not all the members share the same characteristics.[600] This means that the characteristics assigned to the group (and to the individual as a member of the group) may not be applicable to each individual in the group.[601] As a result, an individual may be identified as a member of the group but he/she cannot be identified as a single entity. This is because the creation of a non-distributive group profile is not based on the personal data of identifiable individuals but on the data (often anonymous) of other individuals.[602] In other words, the data used to create the profile are not the personal data of the classified individual but rather derive from the categorisation and generalisation of a large amount of data collected from a number of other individuals. As a result, the knowledge inferred from the profile is probabilistic: the characteristics assigned to the members of the group are derived from the probability that the members belong to that group and not from the data belonging to them.[603] If, for example, a group of people with certain genetic characteristics indicates that there is 80% probability that its members will suffer from a particular type of disease, this does not mean that every individual in the group has an 80% possibility of suffering from this disease. The fact that an individual has an 80% possibility of suffering from the disease does not result from the data collected about him/her, but from the fact that the individual is a member of that group (in which its members have an 80% possibility of suffering from this disease). As a result, characterising an individual in the group as having this type of disease may not be true.[604]

In this respect, the use of such data cannot qualify as the personal data of an identifiable individual since neither of the two elements of personal data can be satisfied. Consequently, non-distributive profiles are not considered to be within the scope of the GDPR. This implies that not only the individuals whose (personal) data

[600] See section 1.7.1 in Ch 4.
[601] Noberto Nuno Gomes de Andrade, 'Data Protection, Privacy and Identity: Dustinguishing Concepts and Articulating Rights' in Fischer-Hübner et al. (eds), Privacy and Identity Management for Life. Privacy and Identity 2010 IFIP Advances in Information and Communication Technology, vol 352. (Springer, Berlin, Heidelberg 2011) 102–103; See also Ronald Leenes 'Regulating Profiling in a Democratic Constitutional State. Reply: Addressing the Obscurity of Data Clouds' in Mireille Hildebrandt and Serge Gutwirth (eds), *Profiling the European Citizen: Cross-Disciplinary Perspectives* (Springer 2008) 293–300.
[602] Andrade 2011 (n 601) 103.
[603] Yves Poullet, 'About the E-Privacy Directive: Towards a Third Generation of Data Protection Legislation? in Serge Gutwirth, Yves Poullet and Paul de Hert (eds), *Data Protection in a Profiled World* (Springer 2010) 3–30.
[604] Custers 2004 (n 83) 153.

were used to create the profile but also the individuals to whom the profile applies are not protected under the GDPR. In this case, therefore, individuals have no access to and no control over their profiles. Moreover, since the data are not personal, the controller has no obligation to ensure the protection of the data as provided by the GDPR. This, of course, raises questions in relation to the fairness, lawfulness and transparency of group profiles.

Thus, the issue in the case of non-distributive group profiles is not whether the GDPR adequately protects individuals but whether there is any protection at all. Considering the material scope of the Regulation, the answer is obvious: the GDPR, just like the DPD, does not provide protection against the creation and application of non-distributive group profiles.

5.3. Problems Arising when the GDPR Applies

Having examined when the GDPR is applicable, and also the problems that arise from the applicability of the Regulation, the following sections consider the protection of individuals against profiling and its challenges when the GDPR applies. The analysis is made under the assumption that the data processed constitute the personal data of an identifiable individual as explained above.

5.3.1. The Problem with the Data Protection Principles

When the GDPR applies, the processing of data for profiling must be in accordance with the rules of the Regulation. These rules do not prevent the processing of data or the use of profiling, but they set out the conditions for fair and lawful profiling activities. In other words, they try to balance the interests of the parties involved by establishing boundaries between the rights of individuals and the obligations of business entities. However, in practice, the effective application of those rules may lack certainty. For this reason, the following subsections examine how the general principles of the Regulation engage with profiling.

5.3.1.1. Purpose Limitation: Collecting and Re-processing of Data

A specific point of attention concerns the purpose limitation principle. The goal of this principle is to ensure that the processing of data is lawful, fair and transparent. In determining, therefore, whether profiling fulfils these requirements, the way data are collected and how they are intended to be used are important elements.

The principle consists of a two-part test: firstly, the data should only be collected for specified, explicit and legitimate purposes and secondly, these data should not be further processed in a way that is incompatible with those purposes.[605] This means that the controller must explicitly specify the purposes for which he/she intends to use profiling before the collection of the data (general purposes such as for 'marketing strategies' or 'improving user experience' are not sufficient) and that the purposes must be communicated in an intelligible and transparent form for the individual and be lawful under one of the legal bases required by the Regulation.[606]

However, the correct application of this principle is questionable in the context of profiling since the purpose of the profiling may not be known at the time of the collection of the data. As Viktor Mayer-Schonberger and Yann Padova describe it, the collection of the data is 'opportunistic rather than purposeful'.[607] This is because it is after the analysis stage (after the collection) that the real value of the data will be discovered.[608]

As seen in Chapter 1 of this thesis, one of the basic elements of profiling is that it constitutes a hypothesis in the sense that it does not only give answers to existing questions but it also creates answers to new questions that the controller did not know to ask in advance (before the collection).[609] In other words, profiling enables the identification of hidden patterns and correlations in the data that the controller did not intend to discover when collecting the data. In this way, profiling produces

[605] Article 5(1)(b) GDPR.
[606] Article 29 Working Party, Opinion No. 03/2013 (n 490).
[607] Mayer-Schonberger and Padova 2016 (n 75) 320.
[608] Mayer-Schonberger and Padova 2016 (n 75) 319.
[609] See section 1.6.3 in Ch 1.

new knowledge about individuals which gives new value to the data and thus creates new purposes.

Consider, for example, a supermarket that is collecting customers' data (e.g. name, date of birth, contact details, marital or work status etc.) for the purpose of its loyalty card programme. By analysing these data, the supermarket discovers that the majority of its customers who shop on Sundays are university students and young professionals who prefer frozen food. In light of these findings, the supermarket decides to offer discount coupons on certain products (e.g. baby food or birthday cakes) every Sunday, in order to attract other customers as well. This new pattern between the customers was not something that the supermarket intended to discover when collecting the customers' data. Its only intention was to provide the customers with loyalty cards. It follows, therefore, that unless the collected data are analysed, the controller does not know the real value of the data and where such value – new knowledge – will be useful in order to assess the purposes of its collection (i.e. how to apply the profile).

Thus, even if the purposes of the profiling are known in advance, they may change after the analysis stage because new unexpected patterns are found in the data that lead to additional purposes that could not considered in the first place.[610] In the above example, while the customers' data were collected for the loyalty card programme, the analysis of the data reveals information that the supermarket can use for its marketing strategies.

The next issue, therefore, that needs to be considered is the further use of data for other purposes. As indicated above, the second part of the principle does not expressly prohibit re-processing of data for new purposes. It only requires that the data should not be further processed in an incompatible way.[611] This means that where the data are to be used for an incompatible purpose, a new legal basis is required (e.g. an individual should be asked again for his/her consent). Thus, as long as the new purposes are compatible with the initial ones, further profiling is allowed.

[610] Roosendal (ed) 2013 (n 182) 182.
[611] Recital 50 and Article 6(4) GDPR.

In such a case, no new legal basis is required for the profiling to be lawful (e.g. an individual should not be asked again for his/her consent).[612] In this way, the GDPR creates for controllers the flexibility to process data for any other purpose which may be considered as compatible with their initial profiling activities.

In order to determine whether the further profiling is compatible with the initial one, the controller should assess whether such profiling goes beyond the scope of the purposes for which the data were collected. In doing so, the controller must consider the following factors (compatibility test): (a) the link between the initial and the intended further purposes; (b) the context of the collection of the data and the reasonable expectations of individuals based on their relationship with the controller; (c) the nature of the data, the consequences for the individuals and the existence of security measures (e.g. encryption or pseudonymisation).[613]

The first two factors are of particular importance here. There must be some sort of relationship between the initial and further purposes, and the individual can reasonably expect, based on his/her relationship with the controller (e.g. seller–customer or doctor–patient relationship), that his/her data may be used in this way. This seems to suggest that any further profiling activity which is deemed to be reasonable for the individual because of his/her relationship with the controller would satisfy the requirements of the compatibility test and thus be lawful.[614] For example, the customers of the supermarket mentioned above may have reasonable expectation that their loyalty card data may be used by the supermarket for its marketing strategies. Thus, the re-use of the data to provide discount coupons for the customers can reasonably be seen as a usual activity between the supermarket and its customers. Moreover, it could be argued that there is a link between the use of data for providing loyalty cards and the re-use of data for providing discount coupons. This, however, does not mean that every time the supermarket uses the customer's loyalty card data for its marketing strategies, that such use will be within the expectations of the customer and thus considered compatible.

[612] Recital 50 GDPR.
[613] Article 6(4) and Recital 50 GDPR; See also Article 29 Working Party, Opinion No. 03/2013 (n 490).
[614] Waltraut Kotschy, 'The Proposal for a New General Data Protection Regulation – Problem Solved?' (2014) International Data Privacy Law 4(4) 279.

If the processing of data is unexpected, inappropriate or does not meet the expectations of a reasonable person in the situation of the individual, it is likely to be considered incompatible.[615] For example, the use of loyalty card data to provide personalised discounts to customers of a specific region (i.e. racial profiling) or to assess when a female customer is likely to be pregnant in order to send her targeted baby products or pregnancy offers in advance, is unlikely to be the reasonable expectation of the customer.[616] Moreover, the use of data on an individual's social media accounts to make decisions about him/her may also not constitute the reasonable expectation of the individual. If, for instance, a business entity is going to use information that the individual has posted on his/her social media account (e.g. links, photos or video uploads) to assess his/her suitability for a job or credit worthiness, this is unlikely to be either within the expectation of the individual or to satisfy the compatibility test.[617]

Another issue that makes the application of the principle problematic is the predictive-future character of profiling. Profiling does not only provide knowledge about an individual's past and current conditions but it also makes predictions about the probable future situation of the individual.[618] This knowledge can result in unexpected future purposes (e.g. five or ten years after the initial purposes). Consider the example of the student loan company mentioned in Chapter 2. The company can use information about its current student loan holders to discover, for instance, their future financial situations.[619] Such knowledge can be used by business entities to offer certain services to them in the future (e.g. a student with future high credit worthiness may be offered a high rate for a future home loan). The question that arises is whether such future purposes can satisfy the compatibility test. In other words, can the students have a reasonable expectation that their data (collected for a student loan application) can be used to assess their future suitability for a home loan or to calculate their rate for a future loan, or should such purposes be considered to be incompatible with the initial purpose to grant a student loan (e.g. five or ten years before)?

[615] Article 29 Working Party, Opinion No. 03/2013 (n 490).
[616] ICO 2014 (n 15) 22; See also Article 29 Working Party, Opinion No. 03/2013 (n 490).
[617] ICO 2014 (n 15) 22; See also Article 29 Working Party, Opinion No. 03/2013 (n 490).
[618] See section 1.6.2 in Ch 1.
[619] See section 2.2 in Ch 2.

In analysing the purpose limitation principle, the Article 29 Working Party directly addresses the issue of the compatibility test in relation to profiling and big data analytics. It identifies two types of compatible further purposes: firstly, when profiling is done to predict general trends and correlations in the data, and secondly, when profiling is done to analyse or predict the preferences, behaviour and attitudes of individuals in order to make decisions affecting them (e.g. to provide personalised offers or targeted advertisements).[620] In this context, it can be argued that the Article 29 Working Party allows a broad range of profiling activities to be considered compatible.

In the first case, emphasis is given to the technical and organisational measures the controller should apply in order to ensure the security and confidentiality of the data (e.g. anonymisation or psedonymisation). In the second case, the Article 29 Working Party requires that the free, specific, informed and unambiguous opt-in consent of the individual is necessary in order for the further profiling to be lawful, and demands that the controllers provide individuals with access to their profiles.[621] Additionally, the Article 29 Working Party states that further processing for different purposes does not automatically render the profiling incompatible but that it should be assessed on a case-by-case basis.

The meaning of *incompatible purposes* is not further defined in the GDPR. However, the Regulation sets out the conditions under which further profiling is permitted, even if the purpose of such profiling is incompatible with the initial one. The first way for controllers to process data for incompatible purposes is by obtaining the individual's consent for the profiling or if the profiling is based on an EU or Member State law.[622] The second way is when the profiling is for archiving purposes in the public interest or for scientific, historical research or statistical

[620] Article 29 Working Party, Opinion No. 03/2013 (n 490).
[621] Article 29 Working Party, Opinion No. 03/2013 (n 490); See section 5.4 below for a detailed analysis of consent.
[622] Article 6(4) GDPR.

purposes (hereafter 'statistical purposes').[623]

Under the DPD, further processing for statistical purposes could only take place if the Member States adopted suitable legal measures which permit such processing.[624] The GDPR does not follow this supposition but it creates an exception to the principle:[625] further profiling for statistical purposes is allowed without the need for a new legal basis (e.g. the individual's consent is not required) as long as the controller adopts 'appropriate safeguards'.[626] This shows that, on the one hand, the GDPR tries to restrict the flexibility of controllers to process data for any other purposes and, on the other hand, it attempts to narrow such restrictions.

As mentioned in Chapter 4, the term 'statistical purposes' is given a broad meaning, including the processing of data for public and commercial interests alike.[627] In the Regulation, statistical purposes are defined as 'any operation of collection and the processing of personal data necessary for statistical surveys or for the production of statistical results'.[628] In the dictionary, *statistical* is defined as '(…) consisting of, or based on statistics';[629] and *statistics* is defined as 'the science that deals with the **collection**, **classification**, **analysis**, and **interpretation** of numerical facts or data, and that, by use of **mathematical theories** of **probability**, imposes order and regularity on aggregates of more or less disparate elements'.[630]

Arguably, the definition of *statistics* coincides with the meaning of profiling and the six steps of the Knowledge Discovery in Databases (KDD) process as explained in Chapter 1 of this thesis: profiling involves the collection and (statistical) analysis of data, with the use of data mining techniques (i.e. mathematical algorithms), in order to identify and classify probable patterns and correlations of behaviour in profiles.[631]

---

[623] Article 5(1)(b) GDPR and Recital 50; see also Recitals 159, 160 and 162 for the meaning of scientific, historical and statistical research. It should be noted that the public health research is treated as a subject of scientific research.
[624] Recital 29 DPD.
[625] Kotschy 2014 (n 614) 281.
[626] Article 89(1) GDPR.
[627] Recital 159 GDPR.
[628] Recital 162 GDPR.
[629] Dictionary.com, <http://www.dictionary.com/browse/statistical> (accessed 27 November 2016).
[630] Dictionary.com, <http://www.dictionary.com/browse/statistics> (accessed 27 November 2016).
[631] See section 1.8 in Ch 1.

Clearly, therefore, profiling reflects what *statistics* is all about. So viewed, it seems difficult not to argue that the processing of data for profiling would not form (in almost all cases) processing for statistical purposes under the GDPR. Interestingly, this would mean that any further profiling activity can fall within the exception of statistical purposes of the GDPR and thus be considered to be compatible and lawful, without the need for individual's additional consent.[632] In this way, it can be argued that the GDPR gives *authorisation* to business entities to re-process data for profiling, for any other purposes and without restrictions, by simply claiming the exception of statistical purposes. In light of this argument, however, it is questionable whether the exception of statistical purposes will remain an exception or whether it will become the general rule, allowing business entities to legitimise their otherwise incompatible profiling activities.

According to Article 5(1)(b) GDPR, further profiling for statistical purposes must be in accordance with the conditions and safeguards referred to in Article 89(1) GDPR. Article 89(1) GDPR provides that the controller must adopt technical and organisational measures in order to ensure the rights of individuals and, in particular, the principle of data minimisation. However, it does not further clarify what these measures should be. It only states that such measures may include the use of pseudonymisation or anonymisation, provided that the statistical purposes can be fulfilled in this way. Unlike anonymous data, pseudonymous data continue to be protected under the GDPR. In contrast, where data are anonymised, they fall outside the protection of the Regulation (unless the individual can be re-identified with the use of reasonable effort). This enables the controller to use the data for a longer period of time without being subject to the rules of the Regulation.

Nevertheless, if statistical purposes cannot be fulfilled by processing pseudonymous or anonymous data, the article permits the processing of personal data for those purposes. In this case, the GDPR authorises Member States to adopt measures to

[632] A good example is that of a company producing internet-connected sex toys. The company by using the argument of 'market research purposes' has continuously collected data about the temperature and vibration intensity of the toys while they are being used by the users (without their consent) in order to understand what settings and levels of intensity are most preferable (Anthony Cuthbertson, 'Is Your Sex Toy Spying on You?' (8 November 2016) Newsweek <https://www.newsweek.com/your-sex-toy-spying-you-489328> (accessed 15 January 2017)).

ensure that the processing of personal data does not affect a particular individual, as well as to provide derogations for the rights of individuals (as provided under Articles 15, 16, 18, 19, 20 and 21 of the GDPR) if the exercise of such rights 'seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes'.[633] In this way, it is to be contended that the protection of individuals is overridden by the priority of controllers to process data for statistical purposes (or otherwise profiling).[634]

Consequently, therefore, Article 89 GDPR does not effectively ensure the efficacy of the Regulation to protect individuals where the exception of statistical purposes applies.[635] This is, firstly, because as long as the controller uses anonymous data, these data can be further processed for statistical purposes (meaning, for a broad range of profiling activities); secondly, because the article permits the use of personal data without requiring the consent of the individual; and thirdly, because the article does not state who can re-process the data for such purposes: is it only the controller who initially collects the data or can the data also be transferred to a third party for these purposes? In the first case, the controller is chosen by the individual and is likely to be someone he/she trusts (e.g. credit scoring is done by the individual's bank) while in the second case, the controller is unknown to the individual (e.g. the credit scoring is done by a credit scoring agency).[636]

Additionally, the fact that Article 89(1) GDPR does not define the types of measures that should be adopted, but leaves it up to the choice of each Member State, is problematic. This is because some Member States may adopt flexible measures in order to encourage profiling activities while others may adopt more restrictive ones.[637] As a result, controllers will have to deal with different measures across the EU and individuals with different levels of data protection. Arguably, this will impair the effect of the GDPR as a harmonised data protection legal instrument for

[633] Recital 156 and Article 89(2)–(3) GDPR.
[634] Kotschy 2014 (n 614) 281.
[635] Kotschy 2014 (n 614) 281.
[636] Kotschy 2014 (n 614) 281.
[637] Mayer-Schonberger and Padova 2016 (n 75) 327.

profiling in Europe.[638]

5.3.1.2. Minimisation and Accuracy of the Data

The next problem concerns the principles of data minimisation and accuracy. According to the general data protection principles, controllers should limit the amount of data they collect and process and must keep the data accurate. In particular, the GDPR requires that data must be 'adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed' (data minimisation principle) and that the data must be 'accurate and kept up to date' (accuracy principle).[639]

Like the DPD, the GDPR maintains the data minimisation principle but it attempts to make it stronger by requiring that the data should be 'limited to what is necessary' for the purpose of the profiling. In short, no more data that are necessary should be used. In terms of profiling, however, this is antithetic. The idea of profiling is to collect, combine and analyse vast amount of different types of data from a variety of data sources. In essence, profiling is about collecting and analysing as many data as possible.[640]

Viktor Mayer-Schönberger, a professor at Oxford University, and Kenneth Cukier, the senior editor for Data and Digital at *The Economist*, speak about the 'N=all' approach which requires the analysis of all the data in the database(s).[641] They argue that '[i]n order to fully investigate an individual, analysts need to look at the widest possible penumbra of data that surrounds the person – not just whom they know, but whom those people know too, and so on'.[642] This means that business entities do not use a sample of data to make their analysis (e.g. to identify a customer's preference) but rather all the data available about a particular individual. For example, if an internet service provider wants to automatically offer to its users discount coupons

[638] Mayer-Schonberger and Padova 2016, (n 75) 327.
[639] Article 5(1)(c) and (d) GDPR.
[640] ICO 2014 (n 15) 23.
[641] Charles Duhigg, 'How Companies Learn Your Secrets' (16 February 2012) New York Times <https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html> (accessed 10 October 2016).
[642] ICO 2014 (n 15) 23.

for stores and restaurants based on their current geographical locations, it needs to have a wider picture of its users, not just to know their current locations but also their preferences and lifestyle (e.g. food preferences, shopping and spending habits, most visited restaurants and stores etc.).

From a data minimisation perspective, however, this creates questions as to whether the data processed are (unreasonably) excessive and also whether all these data are relevant to what is necessary for the purpose of the profiling (e.g. to provide discount coupons for stores and restaurants in the users' current geographical locations).[643] This is especially an issue in the case of autonomic profiling (i.e. AmI and IoT) where, by default, every piece of data is collected and stored somewhere.[644]

Yet, as it is shown in Chapter 2, profiling may reveal new unexpected patterns and correlations that may give new personal data about individuals and their lives. The use of facial recognition technology, for example, to assess the emotional reactions of customers during the demonstration of a product, may disclose correlations between customers' clothing tastes and their emotional reactions. This information is not necessarily relevant to what is necessary for the purpose of creating customers' emotional profiles related to the product.

The question, therefore, that arises is: what constitutes necessary collection of data in the case of profiling? The GDPR does not clarify what the term *relevant and limited to what is necessary* means. Is, for example, the continuous tracking of all individuals' activities through the internet 'limited to what is necessary' for an online store to offer targeted advertising for its products?; is the collection of data from individuals' social media accounts 'relevant' to the bank for assessing their suitability to pay their debts?; or is the collection of an employee's data relating to his/her visits to a psychologist 'relevant and limited to what is necessary' for the employer to determine if the employee is suitable for a job or a promotion? One way for the controllers to know what data are relevant and not excessive to the profiling is to identify the purposes of the profiling before the collection of the data. However,

[643] ICO 2014 (n 15) 23.
[644] Rouvroy 2008 (n 459) 39.

as it is explained above, the purpose of profiling cannot be known unless the data are analysed. Consequently, if the controller cannot determine the purposes of the profiling before the collection of the data, how can he/she assess what data will be relevant for a certain profiling?

Furthermore, the accuracy of the profiling may also be an issue. The GDPR provides that the data must be 'accurate and kept up to date' (accuracy principle).[645] Theoretically, for a profile to be accurate the controller must collect as many data as possible about the individual subject. By contrast, data minimisation requires the limitation of the data to the extent necessary. As a consequence, such limitation may create problems as to the accuracy of the profiles. In terms of profiling, therefore, the application of the data minimisation principle is debatable since the more data are collected for the creation of profiles the more accurate the result of the profiling will be (i.e. the application of the profile will be more precise).[646]

As a result, the strict application of the principle may create less accurate profiles which may lead to the challenges described in Chapter 2. In particular, inaccurate profiles may increase the false positive and false negative results of profiling and thus facilitate unfair treatments of individuals (e.g. discrimination, stigmatisation, stereotyping and de-individuation). In this context, it can be argued that the GDPR cannot be seen as an effective legal instrument against discrimination because the data minimisation principle will not necessarily prohibit or eliminate the discriminatory effects of profiling.

5.3.1.2. Retention of the Data

A third problem relates to the storage limitation principle. According to this principle, controllers should also limit 'to a strict minimum' the period of time they store the data.[647] The GDPR, however, does not further explain what the term *strict minimum* means or how it should be assessed. It only provides that the data must be

[645] Article 5(1)(d) GDPR.
[646] Hildebrandt 2009b (n 184) 245; See also Schermer 2013 (198) 147.
[647] Recital 39 GDPR.

kept 'for no longer than is necessary for the purposes for which the personal data are processed'.[648] In other words, the data can only be retained for the period necessary for the completion of the initial profiling for which they have been collected. In this way, the Regulation gives flexibility to controllers to determine for themselves what is the 'strict minimum' period for each of their profiling activities. In addition, further storage of the data for other purposes presupposes a new legal basis (e.g. an individual must give his/her consent or the retention must be in the legitimate interest of the controller).[649]

In the same way as with the purpose limitation principle, the GDPR provides an exception to the storage limitation principle. It allows for further retention of data, for longer than is necessary and without the need of new legal basis, insofar as the data will be processed solely for statistical purposes and in accordance with the safeguards of Article 89(1) GDPR (as well as of the security measures adopted by the Member States as provided under Articles 89(2) and (3) GDPR). Once more, the Regulation leaves room for controllers to retain the data for longer periods for statistical purposes.

Bearing in mind, however, that the majority (if not all) of profiling activities constitute processing for statistical purposes, it is obvious that the GDPR encourages business entities to retain the data beyond the initial period and (re-) use these data for their future profiling activities.[650] Take, for instance, the example of the student loan company mentioned in Chapter 2.[651] By arguing the statistical exception, the company can retain the data of its current student loan holders (collected for student loan applications) and (re-) use these data for any future profiling activity, without the consent of the student loan holders. Considering, therefore, the statistical purposes exception as well as the capacity of profiling technologies to store a large amount of data with almost no cost, the flexibility of further retention may lead controllers to keep the data forever.

[648] Article 5(1)(e) GDPR.
[649] Article 6(4) GDPR; See also Mayer-Schonberger and Padova 2016 (n 75) 330.
[650] Mayer-Schonberger and Padova 2016 (n 75) 330.
[651] See section 2.2 in Ch 2.

To summarise, the data protection principles aim to ensure that profiling is lawful, fair and transparent. For this reason, the principles attempt to safeguard the individuals' right to control who is going to process their data, for how long and for what purposes as well as to enhance the accountability and transparency of controllers in the profiling. However, following the above analysis, it can be argued that the effective application of data protection principles is not objective in the context of profiling since, as it is shown, it is difficult to ensure total compliance with those principles.

The GDPR requires controllers to limit the collection, (re-) processing and retention of data to what is strictly relevant and necessary for the purposes for which they are collected. By contrast, profiling involves the collection and retention of as much data as possible and for longer periods of time. In addition, the transformative nature of the value of the data makes the purposes of the profiling unforeseeable at the time of the collection. As such, it is uncertain how these principles will be correctly and effectively applied, especially in the case of autonomic profiling (i.e. AmI and IoT environments) where, by default, every piece of data is collected and stored somewhere.[652]

To mitigate, however, this contradiction, the GDPR provides for controllers a number of flexibilities for the re-processing and retention of data. It allows the controllers to keep and process data for longer periods and for a number of different purposes, provided that these purposes are compatible with the initial ones or fall within the exception of statistical purposes. This suggests, however, that as long as the profiling is compatible or done for statistical purposes, the data can be kept and processed forever. Bearing in mind that 'statistical purposes' reflects what profiling is all about, the GDPR indirectly gives to controllers the *authority* to use the retained data for any of their profiling activities and without the additional consent of the individual. Moreover, if the controller complies with consent or other legal basis or if he/she includes the new (incompatible) purposes or the further retention of the data within the context of statistical purposes, the limitation requirements are abolished.

[652] Rouvroy 2008 (n 459) 39.

What is more, if he/she chooses to anonymise the data, he/she will be free, from any obligation under the GDPR, to retain and process the data for an unlimited period. In the end, the GDPR does not intend to restrict profiling activities but rather to offer ways to enable further profiling.

The principles that have been analysed above show that the GDPR presents many gaps and cannot create a symmetry between the business entities and the individual data subjects. Obviously, all the above open-ended restrictions, in relation to further processing and retention of data, leave room for different interpretations of the principles and create problems as to the transparency, lawfulness and fairness of profiling.[653] Perhaps the most important issue is the lack of certainty in relation to the lawfulness of profiling, which may create problems with the legal basis of consent. For this reason, consent will be examined hereafter.

5.4. Consent: Real Choice or Pseudo-Right?

As it is stated in Chapter 4, profiling is subject to the rules governing the legal basis for the processing of personal data under the GDPR.[654] This means that profiling can only take place if it is justified under one of the legal bases specified in Article 6(1) GDPR.[655] Although the consent of the data subject is only one of the legal bases provided under Article 6(1) GDPR, in practice it is the basis most commonly used by business entities to justify their profiling activities.

Perhaps the most disputable issue in the GDPR is the legal basis of data subject's consent. The Regulation recognises consent as the primary legal basis for the processing of individuals' personal data.[656] Liam Curren and Jane Kaye describe consent as 'the making of a voluntarily decision, by a competent individual, to allow an act to occur that may have been impermissible, absent the consent'.[657] In other

[653] Kohnstamm 2014 (n 459) 157.
[654] Recital 72 GDPR.
[655] See section 4.6 in Ch 4.
[656] Ferretti 2014 (n 328) 118.
[657] Liam Curren and Jane Kaye, 'Revoking Consent: A 'blind spot' in Data Protection Law?' (2010) 26 Computer Law & Security Review 274; See also Ferretti 2009 (n 330) 15.

words, consent allows the processing of individuals' data that would otherwise not be allowed.

The idea of consent is to enable individuals to exercise control over their personal data and any decision made based on those data. In this way, the Regulation gives to individuals the means to control aspects of their identities and personalities in order to make free choices and preserve their autonomy and self-determination in society.[658] For this reason, the GDPR requires that individuals must consent not only to the creation of the profile but also to decision-makings based on profiling.

For consent to be valid, it must meet the requirements provided under Article 4(11) GDPR. According to Article 4(11) GDPR, consent constitutes 'any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her'. Therefore, for the consent to be legally justified, the controller must be able to prove that the individual has expressed his/her free, specific, informed and unambiguous agreement to the profiling. If one of the aforesaid requirements is not present, consent is invalid and thus profiling would be unlawful. It should be noted that where profiling is based on the processing of special categories of data (i.e. sensitive and children's data), the consent given should be explicit. The following subsections will examine each requirement separately in order to determine the extent to which they are applicable in practice.

5.4.1. Free Consent

Firstly, consent must be freely given, which implies that the individual must have a genuine and free choice to consent to the profiling.[659] Freely given consent reflects the value of autonomy and the capacity of the individual to make his/her own

[658] Bart Custers et al., 'Informed Consent in Social Media Use – The Gap Between User Expectations and EU Personal Data Protection Law' (2013) 10(4) *Scripted (A Journal of Law, Technology and Society)* 435; See also Curren and Kaye 2010 (n 657) 274.
[659] Recital 42 GDPR.

autonomous choices and live according to his/her own wishes.[660] According to the Article 29 Working Party, consent is freely given when the individual 'is able to exercise a real choice, and there is no risk of deception, intimidation, coercion or significant negative consequences if he/she does not consent'.[661] Therefore, consent must be the result of an independent decision on the part of the individual, free from any influence by others: the individual has to be free to decide for him/herself if he/she wants to consent to the profiling or not.[662] If the individual has no choice but to consent to the profiling (e.g. because otherwise he/she will not have access to a certain service), consent is not freely given since it is not the result of the autonomous choice of the individual.[663]

However, there has always been much debate over whether individuals are in a position to freely choose, or actually make, an autonomous decision. This is because many of the controllers' practices (e.g. technological applications and data collection methods) and the wording used in their privacy policies are so complex that it makes it difficult for the individual to understand the ways in which his/her data are to be used.[664]

Moreover, by providing to the individual inadequate information as to the purposes of the profiling or its possible consequences, it also removes from the individual the ability to make a free choice. To make a free choice, an individual must be aware that he/she will be profiled as well as of the possible consequences profiling may cause to him/her, which implies that he/she must know that he/she may be manipulated, discriminated against, stigmatised and so on.[665] However, in practice, the individual is not aware that he/she is being profiled or that the controller is utilising manipulative or discriminatory techniques to influence his/her choices in a certain way (e.g. to direct his/her decision to buy a certain product instead of another).[666] By notifying the individual that his/her data will be used to provide him/her with personalised services, it does not suggest, from the individual's point of

[660] See section 2.3.3 in Ch 2.
[661] Article 29 Working Party Opinion No. 15/2011 (n 511) 12.
[662] Custers et al. 2013 (n 663) 445; See also Roosendaal 2013 (n 182) 186.
[663] Borghi, Ferretti and Karapapa (2013) (n 513) 123.
[664] Borghi, Ferretti and Karapapa (2013) (n 513) 123.
[665] See Ch 2 for a detailed analysis on the challenges of profiling.
[666] See Zarky's example in section 2.3.3 of Ch 2.

view, that such techniques will take place.

Another problem is that consent may be subject to other conditions. Although the GDPR provides that the individual must give separate consent for different profiling activities and that consent should not be subject to the performance of the contract,[667] in reality, this is often not the case. A common practice today is that many controllers incorporate consent into the terms and conditions of the contract.[668] This means that by accepting the contract, the individual also accepts profiling for other purposes. For example, the individual is only allowed to use a service if he/she also consents to profiling for marketing purposes. In this case, consent to profiling for marketing purposes is a precondition for the individual to accept the terms and conditions (he/she is only allowed to use a service if he/she also consents to profiling for marketing purposes). If the individual does not accept that his/her data is to be processed for marketing purposes then he/she will be denied access to the service. Thus, the individual has no real choice but to accept. Such consent, however, is not freely given because the individual is unable to refuse to give his/her consent without suffering harm (i.e. being excluded from the service).

It should be noted that profiling can be lawful if it 'is necessary for the performance of a contract to which the data subject is party'.[669] However, this legal basis only applies to the profiling that takes place for the performance of the contract (e.g. when the individual requests to use a service or for subscription purposes). In all other cases, profiling has to be based on the legal basis of consent (unless one of the other legal bases provided in Article 6(1) GDPR is applicable). In the example above, the profiling for marketing purposes is not necessary for the use of the service and thus cannot be legitimated under Article 6(1)(b) GDPR. Therefore, by including profiling for marketing purposes in the terms and conditions of the contract, it does not imply that the acceptance of those terms and conditions renders profiling for marketing purposes legitimate under the GDPR. In addition, by including in one document the profiling for other purposes with the profiling that is necessary for the performance

[667] Article 7(2) and (4) and Recital 42 and 43 GDPR.
[668] See, for example, 'WhatsApp' messenger application for smartphones.
[669] Article 6(1)(b) GDPR.

of the contract (use of the service), the controller removes from the individual the right and freedom to make an autonomous decision.[670] This is because if the individual wants to use the service, he/she will accept the processing of his/her data for other purposes.

For this reason, a further element required for consent to be free is that there must be a balance of power between the parties involved. In particular, Recital 43 provides that consent should be considered invalid if there is 'a clear imbalance between the data subject and the controller', specifically where the controller is a public authority. However, the Regulation does not further clarify what exactly constitutes 'a clear imbalance'.

In speaking about consent in terms of contract law, Stephen Smith argues that consent is free and voluntarily given not only in the absence of pure states of necessity, but also in the absence of substantively unfair contract terms.[671] In other words, for consent to be free the contract must be fair for the individual. This would mean that the individual must be in an equal bargaining position with the business entity before consenting to the contract.[672] In terms of data protection legislation, this suggests that profiling must be fair and that the individual must be in a strong bargaining position to effectively control the use of his/her data before providing his/her consent.[673] To determine, therefore, whether there is a clear imbalance between the individual and the controller, it should be examined if consent is fair and whether the individual is in an equal bargaining position with the controller.

Nonetheless, in practice, there may be many cases where there is a clear imbalance between the individual and the controller. As shown above, in many situations consent is a condition of the contract. Although, in theory, the individual has the right to reject the profiling, if he/she does so, he/she may suffer harm. For example, a customer may be able to refuse profiling for targeted advertising purposes but the

[670] Roosendaal 2013 (n 182) 186.
[671] Stephen A. Smith, *Contract Theory* (Oxford University Press 2004) 331–33.
[672] Sheldon Leader, 'Inflating Consent, Inflating Function, and Inserting Human Rights' in Janet Dine and Andrew Fagan (eds) *Human Rights and Capitalism* (Edward Elgar 2006) 28–47.
[673] Philip E Agre, 'Introduction' in Philip E Agre PE and Marc Rotenberg (eds), *Technology and Privacy: The New Landscape* (MIT Press 1997) 1–28.

result may be that he/she is refused a service or receives it at a lower quality.

A further situation is when the individual may feel dependent on the controller because of the relationship they have (employment or medical relationship) and might fear different treatment if he/she does not provide consent.[674] For example, a patient may fear that he/she will receive poor medical treatment if he/she does not consent to profiling for medical research. In both examples, neither the customer nor the patient voluntarily decides to provide his/her consent. The consent was the result of the fear of losing the service or receiving a lower quality of service. Thus, the consent given cannot be considered either fair or free because the parties involved were not in an equal bargaining position.

In addition, as seen in Chapter 2, in most cases individuals do not know the consequences of the profiling and the extent to which it may challenge their lives. Not knowing the consequences of the profiling suggests that individuals are not in an equal and strong power position to bargain the use of their data and their consent cannot be fair and freely given. For instance, if a user of a dating site was aware that he/she may be stigmatised, would he/she have consented to personalised dating services?; if a supermarket customer knew that he/she may be subject to discriminatory pricing, would he/she have consented to profiling for marketing purposes?; if a user of a social media site knew that his/her posted photos may be used by a potential employer to evaluate his/her suitability for a job, would he/she have chosen to have his/her profile publicly available? In all of these cases, the relationship of the individual with the controller (i.e. dating site, supermarket and social media site) is not fairly in balance since there is a lack of knowledge on the part of the individual as to what harm profiling may cause to him/her.

To conclude, consent is generally not freely given in the context of profiling. Even though controllers can argue that consent is the free and independent choice of the individual, in the sense that no forcible mechanisms were in place to make the individual accept the profiling, in practice, the individual has no genuine option to

[674] Article 29 Working Party Opinion No. 15/2011 (n 511) 13.

make an autonomous decision about the profiling because he/she may not have a clear understanding of the use of his/her data or the consequences of such use in his/her life. What is more, if the individual has no option but to consent to the profiling because otherwise he/she will suffer harm, then the individual is deprived of any right or freedom to choose autonomously and his/her choice cannot be considered as freely given.[675] Ultimately, therefore, such choice can affect the fairness and validity of consent and its effectiveness as a control mechanism in the hands of individuals.

5.4.2. Informed Consent

The second requirement for consent is that it must be informed. Informed consent presupposes that the individual who is giving the consent has a good understanding of what profiling involves, as well as of the consequences of providing his/her consent. In other words, the individual must understand how the controller is going to use, disclose, transfer, and store his/her data and the results of the profiling (i.e. how the profile will apply). For this reason, the individual must be properly informed about the profiling before the collection of his/her data and the information must be precise and understandable in order to enable the individual to make a free and autonomous decision about the use of his/her data.[676]

Properly informed consent means that the individual must be aware of the identity of the controller and the purposes for which profiling is intended to be used.[677] The individual must also understand which of his/her data are to be collected and processed as well as of the potential consequences of the profiling and how they may affect him/her.[678] Additionally, the individual must be notified about his/her rights and his/her ability to withdraw his/her consent at any time.[679]

---

[675] Leader 2006 (n 672) 28–47.
[676] Custers et al. 2013 (n 658) 445, 448; See also Roosendaal 2013 (n 182) 187; Borghi, Ferretti and Karapapa (2013) (n 513) 122.
[677] Recital 42 GDPR; See also Article 14 GDPR.
[678] Recital 42 GDPR; See also Custers et al. 2013 (n 658) 445; Borghi, Ferretti and Karapapa (2013) (n 513) 122.
[679] Article 7(3) GDPR.

However, as it will be seen below, properly informed consent is not always feasible in practice. As already shown, the purpose of the profiling is not always known at the time of the collection of the data. The combination, retention and further processing of data by different controllers can produce new knowledge from the data, the use of which cannot be foreseeable at the collection stage. This means that the controller does not have a good knowledge of the purposes of the profiling and thus he/she cannot properly inform the individual about the exact purposes for which the data are intended to be used. Additionally, not knowing the purposes in advance implies that the consequences of the profiling cannot be assessed either by the controller or by the individual. As a result, the individual will not be able to understand all the effects that the profiling may cause to him/her.[680] In the absence, therefore, of clear purposes (how the profile will apply), the consequences of the profiling are unforeseeable and thus informed consent cannot be achieved.[681]

It should be noted here that where the purposes of the profiling are changed, the individual must also be informed of the new purposes and the further profiling (Article 14(4) GDPR). In many cases, however, controllers do not notify the individual about any changes in their policies. Rather, they encourage the individuals to continue reading the policies and they only notify the individual if they consider the change significant based on their discretion.[682] In such cases, it does not mean that the controller is not complying with the requirement of the Regulation but that the information is inaccurate and inadequate to enable the individual to provide his/her informed consent.[683]

Another situation with informed consent is that the information provided must be understandable, precise and accessible for the individual. Unlike the DPD, the GDPR requires that the information should be in 'an intelligible and easily accessible form, using clear and plain language and it should not contain unfair terms'.[684] Thus, if the

[680] Roosendaal 2013 (n 182) 187.
[681] Roosendaal 2013 (n 182) 158.
[682] Google, for example, states in its policy that '[w]e will post any privacy policy changes on this page and, if the changes are significant, we will provide a more prominent notice (including, for certain services, email notification of privacy policy changes)'.
[683] Borghi, Ferretti and Karapapa (2013) (n 513) 138.
[684] Recital 42 GDPR; See also Article 29 Working Party Opinion No. 15/2011 (n 511) 13.

individual has difficulties in accessing or understanding the information (e.g. the privacy policy is hidden somewhere in the website or is too technical or complicated), consent cannot be informed under the GDPR.

However, whether the information is understandable and precise for the individual is a highly disputable issue. In most cases, privacy policies or terms and conditions are too long and unclear or are provided in a very technical or legal way. Google's and Apple's privacy policies, for example, are about 3000 words long and use various technical and legal terms which are not easily understood by an average user (unless the user is familiar with those terms because of his/her profession or educational background).[685]

Yet, both business entities refer their users to various other links with additional information for the better understanding of their privacy policies. Only a small number of users, however, read this information before accepting the policies. Rather, most users tick consent boxes without reading or understanding the privacy policies. From the user's perspective, this might seem reasonable: how can a person read a 3000 word document for every website, application or service he/she wants to use or product that he/she may want to buy?[686] Even in cases where the user does read the privacy policy, it does not necessarily mean that he/she completely understands the information and the ways in which his/her data will be used. This means that not all the individuals really know what they have consented to.

This is also indicated by the EU's research project named CONSENT.[687] According to the project's results, the majority of the respondents (73%) do not read privacy policies and terms and conditions. In particular, the project indicated that most respondents never (27%), rarely (27%) or sometimes (23%) read these policies. In addition, of those respondents who do read the policies, only 21% completely

[685] See Google's and Apple's privacy policies at <https://www.google.com/policies/privacy/> and <http://www.apple.com/legal/privacy/en-ww/> (accessed 8 January 2017).
[686] Bert-Jaap Koop, 'The Trouble with European Data Protection Law' (2014) International Data Privacy Law doi: 10.1093/idpl/ipu023. <https://ssrn.com/abstract=2505692> (accessed 2 June 2016).
[687] The project examined how consumer behaviour and commercial practices are changing the role of consent in the processing of personal data ('CONSENT project' results (14 October 2014) <http://www.consent.law.muni.cz/> (accessed 8 January 2017)).

understand the context provided whereas 42% said that they understand most parts of the context. If, therefore, individuals do not read the information or they read it but they do not understand it, consent cannot be regarded as properly informed according to the GDPR. As such, non-properly informed consent cannot be regarded as the autonomous and independent choice of the individual.

The last condition for informed consent is that the individual must be aware which of his/her data are to be collected and processed in order to make his/her decision (e.g. if the collected data are sensitive the individual may refuse to give his/her consent). In a profiling context, this is debatable. This is because, as seen in Chapter 2, profiling technologies facilitate continuous and real-time surveillance of individuals. This means that business entities can trace and collect almost all data relating to the individual's activities whether online or offline (e.g. location data, voice data, image data, biometric data etc.).[688] In most cases, therefore, the individual will not be able to know which of his/her data are to be collected and by which controller.

For example, when creating a social media account, it may be clear to the individual which of his/her data are to be collected (e.g. name, date of birth, email address or what books or music he/she likes). If, however, the social media site collects data indirectly (which it is often the case), by tracking the individual's visits to other websites (e.g. Facebook can know all the websites visited by its users as well as of their activities on those websites), this makes it more difficult for the individual to understand which of his/her data are actually being collected. Furthermore, the combination of all these data can reveal new data about the individual which sometimes he/she may not know about him/herself (e.g. the individual is likely to be involved in an accident because of his/her driving speed or to develop an aggressive behaviour because of the movies he/she chooses to watch).

In addition, many privacy policies are too general and do not help the individual to understand exactly what data are to be collected. Google, for example, contains in its privacy policy the following statement: '[w]e collect information to provide better

[688] See section 2.3.1 in Ch 2.

services to all of our users – from figuring out basic stuff like which language you speak, to more complex things like which ads you'll find most useful, the people who matter most to you online, or which YouTube videos you might like'.[689] Although this statement is written in simple wording and provides examples for the better understanding of the user, it does not necessarily mean that the user will understand exactly the volume or the types of his/her data which will be collected.

To conclude, individuals are often not able to give informed consent in the context of profiling. Even where the controller provides, to the individual, all the necessary knowledge to make an informed decision, if the individual does not read or does not understand the information provided, consent cannot be considered to be properly informed. This is because the lack of a sufficient understanding of the profiling and its consequences reduces the individual's capacity to make an autonomous decision. Thus, being informed does not necessarily mean that the consent given is the autonomous decision of the individual.

5.4.3. Specific Consent

The third requirement of consent relates to the principle of purpose limitation. Consent must be specific, meaning that the individual must be aware of the specific purposes for which profiling is taking place before giving his/her consent. In other words, the individual has to agree to a specific profiling that is taking place for specific purposes.[690] For this reason, Article 6(1)(a) GDPR explicitly provides that consent must be given 'for one or more specific purposes'.[691] Therefore, open-ended or all-inclusive consent that covers any possible future profiling purposes is prohibited under the GDPR.[692] In this way, the GDPR tries to ensure that controllers will not rely on the consent basis to use the individual's data for unlimited purposes.

Nevertheless, specific consent may also be questionable if the exact use of the data

[689] See, for example, Google's privacy policy at <https://www.google.com/policies/privacy/> (accessed 8 January 2017).
[690] Article 6 GDPR.
[691] Article 6(1)(a) GDPR.
[692] Article 29 Working Party Opinion No. 15/2011 (n 511).

and the purposes of the profiling are not known at the time the consent is given.[693] Additionally, a frequent situation today is that many controllers, although they try to be specific about the ways in which they use individuals' data, still describe the purposes of the processing in a very general way for the individual. Such purposes are either too short and general or too long and detailed.

In the first case, for instance, statements such as *the data is being collected for the improvement of the service* or *for research and statistical purposes*, do not necessarily mean that they are informed, specific or clearly understandable by all the individuals who want to use the service. Consider the example of a company producing internet-connected sex toys.[694] For the purpose of market research, the company collected users' data about the temperature and vibration intensity of the toys while they were being used. The question that arises is whether the users really understand that the phrase 'for market research purposes' covers also the collection of their data relating to the levels of intensity they most enjoyed when using the sex toy, as well as of the consequences of such collection (e.g. the possibility of a third party intercepting the data and taking control of the sex toy while it is being used by the user, resulting in the user's potential sexual assault) in order for their consent to be specific and informed.

Moreover, many controllers write in their privacy policies that data may be processed for legitimate purposes but they do not further explain what those purposes can be. This does not mean, however, that all individuals have the knowledge to understand what those purposes can be (or the extent to which those purposes will require the use of their data) in order to provide specific consent. Another example is when a controller may provide, in its policy or terms and conditions, that the individual's data will also be transferred to third parties or its partners without specifying who these parties or partners are. Although in these cases, consent may be deemed to be informed, it cannot be specific unless the

[693] Borghi, Ferretti and Karapapa (2013) (n 513) 123; See also Article 29 Working Party Opinion No. 15/2011 (n 511).
[694] See n 632 in this chapter.

individual consented to a specific transfer to a specific party.[695]

In the second case, although the controller may provide to the individual (in detail) a number of different activities for which his/her data can be used, and consent may be deemed to be informed, this does not mean that all of this information is specific and understandable for the individual.[696] On the contrary, the information is so long and detailed that it can be argued that it covers the collection of any of the individual's data and for any purposes. According to the Article 29 Working Party, '[t]o be specific, consent must be intelligible: it should refer clearly and precisely to the scope and the consequences of the data processing. (…) This means in other words that the context in which consent applies is limited'.[697]

Added to that, Recital 43 provides that when the profiling has different purposes, separate consent should be given for each of them in order for the consent to be free and specific.[698] This means, for instance, that if a customer consented to the collection of his/her data for the opening of his/her bank account, it does not mean that the bank can rely on this consent for its other activities (e.g. to also use the customer's data for its marketing purposes). Separate consent should be given for other purposes unless the further use of the customer's data falls within the exception of statistical purposes or is compatible with the initial purpose of opening a bank account (e.g. to examine the customer's eligibility for loan or overdraft facilities). In addition, consent that is necessary for the performance of a contract must be separated from the consent that is needed to process individuals' data for any other purposes. For instance, if a bank's website states that 'by entering your information you consent to the terms and conditions and privacy policy of the bank', it does not mean that the individual also consented to the transfer of his/her data to the partners of the bank (e.g. an insurance company with whom the bank is cooperating).

To summarise, consent cannot be a valid ground for profiling if the purposes for which the data are collected are not specified before consent is given. In practice,

[695] Borghi, Ferretti and Karapapa (2013) (n 513) 139.
[696] See, for example, the privacy policies of Viber and Google Applications or their websites.
[697] Article 29 Working Party Opinion No. 15/2011 (n 511).
[698] Borghi, Ferretti and Karapapa (2013) (n 513) 139.

this is often not the case, bearing in mind the way profiling works and the transformative nature and value of the data. As a result, specific consent is difficult to obtain in all circumstances. For this reason, controllers often provide individuals with broad purposes or even multiple purposes that will cover any future use of the data which may be revealed from the mining of the data and will allow them to retain, (re-) use or disclose the data without limitations.

5.4.4. Unambiguous Consent

Finally, consent must be the unambiguous indication of the individual's wishes. There must be no doubt that the individual intended to provide his/her consent to the particular profiling.[699] This presupposes that the individual has to be properly and specifically informed in order to make a free and independent decision about his/her agreement or not to the profiling, otherwise the consent will be ambiguous.[700]

Unambiguous consent requires any indication of a wish by which the individual signifies his/her agreement to a particular profiling activity. In other words, indication is the way in which the individual's willingness to accept the profiling is signified. When is an indication signified? According Article 4(11) GDPR, the indication can be signified by a statement or a clear affirmative action on the part of the individual. Therefore, what signifies the acceptance may constitute any form of behaviour by which the individual's wishes (consent) can be reasonably inferred.[701] For example, an online bookshop asks its customers to provide their phone number in a blank box if they wish to receive regular information about the arrival of new books through text messages. If a customer writes his/her phone number in the box, this will signify his/her acceptance (unambiguous consent) to receive such texts, since the action of writing his/her phone number in the box leaves no doubt for the bookshop owner as to the customer's wish to receive information about new books. Thus, the word *signifies* requires some form of action on the part of the individual. Inactivity or passive behaviour are unlikely to signify the individual's acceptance

[699] Article 29 Working Party Opinion No. 15/2011 (n 511).
[700] Article 29 Working Party Opinion No. 15/2011 (n 511) p. 21; See also Borghi, Ferretti and Karapapa (2013) (n 513) 120.
[701] Custers et al. 2013 (n 658) 447.

since they lack action.[702] For this reason, under the GDPR, silence, inactivity or the mere use of a service do not constitute unambiguous consent since they do not prove any form of action on the part of the individual (no clear indication of individual's wishes).[703]

What is important is that the GDPR does not limit this action to be provided only in writing. It clarifies that a clear affirmative action may include a written or oral statement, including by electronic means, such as ticking a box when visiting a website ('opt-in' consent), choosing technical settings for information society services or another statement or conduct which clearly indicates the individual's agreement to the profiling.[704] Thus, if, for example, the individual clicks an unchecked box on a website that says 'I agree' or 'I consent' (e.g. to receive customised advertisements), he/she has given his/her unambiguous indication to the proposed profiling and consent will be valid. This is the case of 'opt-in' consent where the individual is considered to have given his/her consent by 'opting-in' to the profiling.

A common situation, however, in the online environment, is that many websites and applications consider the mere use of their services as the 'opt-in' consent of the individual (i.e. the individual is giving his/her consent by starting to use the service).[705] As it is mentioned above, the mere use of a service does not constitute unambiguous consent under the Regulation. At first glance, it seems that the GDPR, unlike the DPD, removes the possibility of 'opt-out' or otherwise implicit consent for the controllers. In the case of 'opt-out' consent, the individual is considered to give his/her consent by not signifying his/her refusal of the profiling. For instance, where a checkbox is showed to the individual and he/she is asked to uncheck the box if he/she does not agree that his/her data can be shared with others for marketing purposes ('opt-out' from consent), the non-unchecking of the box cannot be assumed to be the clear indication of the individual's wishes. This is because the lack of not

[702] Custers et al. 2013 (n 658) 447.
[703] Kuner, Burton and Pateraki 2013, (n 520) 2–3; See also Frederic Zuiderveen Borgesius, 'Behavioral Targeting: A European Legal Perspective' (2013) IEEE Security & Privacy 11(1) 84.
[704] Recital 32 GDPR.
[705] The Viber application, for example, states in its policy that '(…) by using our Services, you give us consent to collect, use, disclose, and retain your personal information and other information (…)' (Viber Privacy Policy <https://www.viber.com/en/privacypolicy.html> (accessed 13 January 2017)).

'opting-out' from consent (i.e. not unchecking the box) does not necessarily signify the unambiguous indication of the individual and thus consent cannot be valid.

Nonetheless, the possibility for controllers to choose technical settings for online services (e.g. default data protection settings), as provided in Recital 32, may still leave room for 'opt-out' (implicit) consent practices. The use of these settings is related to the new principle of 'data protection by design and by default' which requires controllers to ensure, by default, the protection of individuals who are using their services (e.g. the use of pre-tick consent).[706] In addition, Recital 32 provides that a clear affirmative action may also involve 'another (…) conduct which clearly indicates (…) the data subject's acceptance' to the profiling'. This suggests that in some cases unambiguous consent, although not directly expressed, may be inferred from or implied by certain conduct or action of the individual. Thus, implicit consent can also be seen as the unambiguous indication of an individual's wishes under the GDPR, as long as the indication (action or conduct of the individual) 'lead[s] to an unmistakable conclusion that consent is given'.[707]

Nevertheless, whether a conclusion can be unmistakable, especially in the online environment, is questionable. The use of default settings, for example, may create uncertainty as to whether the lack of action on the part of the individual is meant to indicate consent and whether such consent can be considered unambiguous. Consider, for instance, the following example: a social media website, by using default settings (e.g. pre-ticked boxes), allows its users' posting information (e.g. comments, photos etc.) to be viewable by the public unless the users tick a different choice (e.g. viewable only to 'friends' or 'close friends'). If a user neglects to tick another choice, he/she is deemed to have consented to have his/her data publicly available. In such a case, however, it is uncertain whether not ticking another choice implies the unambiguous consent of the user to have his/her posting information publicly available.[708]

[706] Article 25 and Recital 78 GDPR.
[707] Article 29 Working Party Opinion No. 15/2011 (n 511) 23.
[708] Article 29 Working Party Opinion No. 15/2011 (n 511) 23.

Another example is Microsoft's Windows 10 computer operating system. Microsoft automatically upgraded Windows 7 users' computers to Windows 10 without their consent. The Windows 7 users were regularly receiving on their computers a notice asking them if they wanted to install Windows 10. Despite the refusal of many users to accept the installation, Microsoft scheduled users' computers to automatically shut down and start updating to Windows 10 at a specific time and date without their knowledge or permission. The only way to stop such an installation was for the users to discover that an automatic upgrade was scheduled and to disable it by themselves. The fact that a user did not 'opt-out' from the installation does not suggest that he/she knew about or consented to it. There was no clear indication of his/her intention to accept or not the installation.[709]

To conclude, unambiguous consent may not always be possible or clear in the context of profiling since, in many cases, controllers prefer to use 'opt-out' consent practices. Such use creates uncertainty as to whether unambiguous consent is given. In addition, if it is to be accepted that implicit consent is sufficient to prove the element of unambiguous indication of an individual's agreement to the profiling, this will impair the effectiveness of consent and, in turn, prevent individuals from exercising full control over their data. Additionally, it can create problems with controllers' obligation to prove that consent was legally obtained.

5.4.5. Explicit Consent

A final issue is the requirement of explicit consent. The GDPR provides that where the profiling involves the processing of sensitive data, consent must be explicit.[710] Like unambiguous consent, explicit consent requires a clear affirmative action on the part of the individual which shows his/her intention to consent or not to the collection, processing or disclosure of his/her data.[711] As previously mentioned, a clear affirmative action may involve a written or oral statement, including by

[709] Steve Peterson, <http://www.huffingtonpost.com/steve-peterson/warning-your-computer-may_b_10099208.html> (accessed 8 August 2018); See also ComputerWorld.com, <http://www.computerworld.com/article/2983633/microsoft-windows/microsoft-pushes-windows-10-upgrade-to-pcs-without-user-consent.html> (accessed 14 January 2017).
[710] Article 9(2) GDPR.
[711] Recital 32 GDPR.

electronic means (e.g. an electronic or digital signature or through the clicking of a button or an icon).[712] Therefore, 'opt-in' consent will satisfy the element of being explicit under the GDPR. This means that the mere clicking of a button or an icon will be sufficient to legitimise the processing of an individual's sensitive data that would otherwise be illegal (as long as the individual is properly and adequately informed about that processing).[713]

In this context, explicit consent may be understood as having the same meaning as unambiguous consent, since both presuppose a clear affirmative action.[714] However, there is a considerable difference between the two. As it is explained above, unambiguous consent can be valid even if it is not directly expressed by the individual but it is suggested by his/her conduct or actions. In other words, inferred or implied consent may still be validated without the need for an 'opt-in' consent box (e.g. not changing the default settings). By contrast, for consent to be explicit, the individual must respond actively to the question (i.e. if he/she accepts the proposed profiling or not) and his/her response must leave no room for confusion as to whether he/she accepts the profiling.[715] This means that there must be no mistake or doubt as to whether consent is given.[716] Accordingly, consent that is implied or inferred will not meet the requirement of explicit consent.[717]

As such, 'opt-out' consent will not satisfy the element of being explicit.[718] Consider, for example, a patient who is notified by his/her doctor that his/her genetic data will be transferred to a medical institute for research purposes unless he/she will refuse the transfer by calling the clinic ('opt-out' from consent). If the patient does not make the call, it does not mean that he/she accepted the transfer. There is no active

[712] Recital 32 GDPR.
[713] For the illegality of 'opt-out' consent in electronic marketing please see *Consent to Advertising by E-Mail and SMS*, Re (VIII ZR 348/06) Bundesgerichtshof (Germany) 16 July 2008, [2009] E.C.C. 27.
[714] It should be noted that the original Commission proposal suggested consent to be explicit in all cases whatever the data processed (either ordinary or sensitive personal data) in order to avoid confusion and ensure consistency in the interpretation of the definition of consent. Because of the divergence of opinions between the Commission, the Council and the Parliament, the final text of the GDPR tried to balance this divergence by providing for both, unambiguous consent for the processing of ordinary personal data and explicit consent for the processing of sensitive data (Proposal for the GDPR (n 27)).
[715] Article 29 Working Party Opinion No. 15/2011 (n 511) 25.
[716] Article 29 Working Party Opinion No. 15/2011 (n 511) 23.
[717] Article 29 Working Party Opinion No. 15/2011 (n 511) 25.
[718] Article 29 Working Party Opinion No. 15/2011 (n 511) 25.

response on the part of the patient to enable the doctor to come to an unmistakable conclusion about the patient's choice and thus the consent cannot satisfy the element of being explicit.

It follows, therefore, that explicit consent is more demanding than unambiguous consent. Even though inactivity or passive behaviour may, in some cases, be possible to suggest the unambiguous indication of the individual, such behaviour cannot be sufficient to validate explicit consent.

5.4.6. Withdrawal of Consent

For individuals to preserve their right to informational self-determination, they have to be able to exercise control over their data even after they consent to the profiling.[719] For this reason, Article 7(3) GDPR provides for individuals the right to withdraw their consent at any time. The withdrawal or otherwise revocation of consent has been described as 'the process that permits an individual to invalidate or modify previously given consent',[720] and should apply to any copy of the individual's data, which may be held either by the controller or by any other third party to which the data were disclosed.[721] In this way, the Regulation attempts to prevent controllers from obtaining unlimited and permanent control over individuals' data.[722]

As mentioned above, consent is valid and informed if the individual is notified about his/her right to withdraw consent. Thus, the controllers must offer to individuals as easily accessible and understandable methods by which to withdraw their consent as the methods provided to give consent.[723] For example, if an individual has consented to receive direct marketing texts with discount offers, the received texts should

[719] Roosendaal 2013 (n 182) 185; See also Koops 2014 (n 686) 3.
[720] Marco Casassa Mont et al., 'On the Management of Consent and Revocation in Enterprises: Setting the Context' (2009) HPL-2009-49 HP Laboratories Technical Reports <https://pdfs.semanticscholar.org/7ec6/0b7f34497dc170e8a4d85ac30263dbe2f697.pdf> (accessed 17 January 2017).
[721] Casassa Mont et al. 2009 (n 720).
[722] Douwe Korff D, 'Comparative Summary of National Laws', *EC Study on Implementation of Data Protection Directive* (Study Contract ETD/2001/B5 3001/A/49) 27.
[723] Article 7(3) GDPR.

include an option to opt-out from these texts. In short, the opportunity to withdraw his/her consent should be offered with each subsequent text.

Additionally, in the case where a service requires the ongoing processing of data (e.g. a controller's service based on the real-time collection and processing of an individual's location data), the Article 29 Working Party states that the controller should regularly remind the individual that his/her data are continuously collected in order to enable him/her to exercise the right to withdraw consent (e.g. the individual should be informed that his/her smart phone has been, will be or can be located).[724]

In practice, however, controllers may ignore the individuals' right to withdrawal. There are cases, for example, where the right to withdraw consent (e.g. 'unsubscribe') is presented in such a way (e.g. the word 'unsubscribe' is written with very small letters at the end of an email) that is not clearly and explicitly noticeable for the individuals. Likewise, although many controllers give the possibility for individuals to stop receiving emails and notifications of direct marketing, they do not actually consider individuals' wishes (who have chosen to unsubscribe) and they keep sending emails and notifications.

It is important to note that the request for withdrawal may not involve all of the data the controller has collected about the individual but it may affect only specific parts of those data.[725] In other words, the withdrawal of consent may refer partially to a specific use of the data and not entirely to all the uses of the data for which consent was given. For instance, a person who has consented to the processing of his/her data to receive marketing messages and notifications of his/her financial transactions, may choose later to withdraw his/her consent to receive marketing messages.

Nevertheless, the withdrawal of consent should not affect the legality of profiling based on the consent given before its withdrawal. This means that, in the example above, the profiling that took place for marketing purposes before the individual withdrew his/her consent (to receive marketing messages), was valid because

[724] Article 29 Working Party Opinion No. 15/2011 (n 511) 33.
[725] Casassa Mont et al. 2009 (n 720).

consent was in place. If, however, the controllers continue to process the data for marketing purposes after the individual withdraws his/her consent, such profiling will be invalid.

Another problem with the right to withdraw consent is when consent is given subject to the performance of the contract. If consent is incorporated into the terms and conditions of the contract, it will not be easy to withdraw, by the individual, because this will mean the cancellation of the contract (i.e. to stop using the service). In this case, the individual may have no option to withdraw his/her consent. Having no option to withdraw consent, the individual cannot make a real and independent choice and thus his/her consent cannot be seen as a freely given, specific, informed and unambiguous indication of his/her wishes.

Consent is valid if all the above requirements are present. However, as seen above, in a profiling context it is difficult to fulfil adequately all the requirements of consent. It is difficult for individuals to exercise control through their consent in all cases or to refuse to give their consent without being rejected by the desired service.

Thus, a question arises about whether the individuals really have a degree of choice, without being denied the service, or whether consent is a pseudo-right which gives pseudo-protection. In view of the above, the individuals cannot refuse to give or withdraw their consent if they are really in need of the service. Thus, in fact, the individuals' privacy and data protection is being infringed on a daily basis by the individuals themselves in being forced to give their consent in order to have a service.

Therefore, in practice and in real life, the individuals do not have either the right or the choice not to give or to withdraw their consent. There are, for instance, cases like lawyers, doctors and bankers in which the individual cannot afford to lose the service. Consequently, consent does not work in a profiling-based environment. In fact, consent is not the correct and effective way to enable individuals to preserve their autonomy and their self-determination. Following this, therefore, consent is only a pseudo-right which gives only a pseudo-protection.

5.5. GDPR in View of Profiling

In the context of profiling, therefore, it is difficult to effectively apply the Regulation. As shown from the above findings, the applicability of the Regulation is limited in view of profiling because there may be cases in which the profile contains non-personal data or anonymous data that cannot facilitate the identification of the individual within the meaning of Article 2(1) GDPR. This is mostly the case with group profiling, and especially of non-distributive group profiles, although in personalised profiling there may also be cases in which the individual subject is not identifiable within the meaning of Article 2(1) GDPR. In these cases, the GDPR does not apply and the individuals do not have any rights upon their data whereas the controllers have absolute control over the data with no obligation to comply with the provisions of the Regulation. So viewed, group profiling is perhaps the most problematic issue under the GDPR since the members of a non-distributive group profile continue to be unprotected under the new data protection regime.

Furthermore, where the identifiability factor is satisfied, which means that profiling is governed by the rules of the Regulation, the situation is not prosperous either. As shown from the above findings, the GDPR neglects to achieve a level of symmetry between individuals and controllers, either in terms of knowledge or in terms of power (control). On the one hand, the general data protection principles of the GDPR do not effectively apply to ensure the transparency and accountability of controllers. The restrictions on further processing and retention of data indirectly give the *authority* to business entities to re-use the data for further profiling, and for any other purposes, without the additional consent of the individual by simply arguing the statistical purpose exception. Moreover, as mentioned above, the data minimisation principle is inconsistent with profiling because firstly, the more data that are collected and analysed the better for the accuracy of the profiles and secondly, it is difficult for business entities to assess, at the collection stage, which data are likely to be relevant for the profiling since the purpose of the profiling cannot be determined before the collection of the data.

On the other hand, consent as the main legal ground for profiling does not work

effectively in the context of profiling to enable individuals to obtain control of their data and, consequently, of the profiling practices applied to them. In practice, individuals do not have a real choice not to give or to withdraw their consent if they want the service but, in contrast, consent under the GDPR is only a pseudo-right which gives only a pseudo-protection.

As a result, the Regulation is unsuccessful in achieving a balanced distribution of powers between the business entities and their data subjects. Indeed, it is to be argued that the distribution of powers is at the expense of individuals and in favour of the controllers, both in terms of knowledge and in terms of power, and thus how they exercise that power. Therefore, without the right level of balance of powers between the parties involved, the protection provided under the Regulation cannot be satisfactory for the individuals.

In addition, there is no protection of the right to privacy, as such, in the GDPR. As is seen in Chapter 4 of this thesis, the wording of the GDPR does not expressly refer to the right to privacy itself but to the right to data protection.[726] Prima facie, this means that the main objective of the GDPR is to protect the right to data protection and not the right to privacy. In this way, the GDPR establishes an independent presence of data protection within legal society away from privacy boundaries. Moreover, privacy is not mentioned in the provisions of the Regulation (e.g. Article 25 GDPR does not refer to privacy by design but to data protection by design and by default). The only reference to privacy is in the preamble of the GDPR whereas Recital 4 refers to the connection between the two rights and states that the Regulation 'respects all fundamental rights, including the respect for private and family life, home and communications (…)'. Nevertheless, it cannot be argued that the GDPR provides even indirect protection to the privacy right given that the preamble of an EU legislation has no binding effect.

It is implied, therefore, indirectly but very clearly that, under the GDPR, the right to data protection is not the same as the right to privacy. This means that the Regulation

[726] See section 4.2 in Ch 4; See also Article 1(2) GDPR.

treats data protection separately from the right to privacy and not as one of its aspects. However, data protection constitutes only one aspect of privacy. By contrast, as it is revealed from the analysis in Chapter 2 of this thesis, profiling creates challenges for individuals not only in relation to their personal data and to any decision made based on their data, but also to all aspects of privacy. As argued by Professors Samuel Warren and Louis Brandeis: the use of devices and methods which enable the recording, storing and distribution of previously private information of individuals in public can lead to the invasion of the 'sacred precincts of private and domestic life'[727] and that not every aspect of a person's life that could be recorded should be allowed to be recorded and distributed.[728]

Indisputably, from the findings of this chapter, the GDPR neither provides adequate and effective protection for individuals and their right to data protection nor does it consider protection of the individuals' right to privacy within the context of profiling.

[727] Warren and Brandeis 1890 (n 324).
[728] See section 3.6.1 in Ch 3.

Conclusion

The new technological developments and the large amount of data in databases present new challenges for individuals and their lives. The use of profiling technologies enables the digitisation of individuals' everyday activities and creates new possibilities for business entities to access various sources with different types of data about their individual targets. The continuous collection, combination and analysis of these data enables the automatic classification of individuals into certain profiles.

The resulting profiles help business entities to identify their targets, to discover knowledge about the various aspects of their lives and to assign to them a certain value in order to decide who should be included or excluded from their services. These decisions, however, are likely to generate certain prejudicial treatments for the individuals that may be detrimental to their lives and their future opportunities.

The significance of profiling rests on the idea of discovering knowledge from a large amount of data that otherwise would be unknown, and the opportunities that derive from the use of such knowledge which entitles decision-makings for the benefit of business entities. This makes profiling a powerful instrument for business entities to discover information about the individuals' past, current and future characteristics and activities. A vital threat, therefore, to privacy and data protection rights arises from the fact that profiling can reveal personal and sensitive information about the individual 'out of seemingly trivial and/or anonymous data'[729] and thus provides to business entities new means of entry into individuals' private lives and to their personal information.

It is obvious that profiling brings serious challenges for the individuals, their privacy and their personal data. These challenges concern surveillance, asymmetries of knowledge, manipulation and threats to autonomy, discrimination, de-individualisation, stigmatisation, stereotyping and inaccuracy in the information and

[729] Hildebrandt 2008b (n 23) 240.

decision process. At the heart of these challenges are the issue of control and the unbalanced distribution of powers between controllers and individual subjects which generate concerns over individuals' autonomy and their right to self-determination.

Privacy and data protection are recognised as legal instruments which protect the rights of the individuals to preserve their freedom to develop their own unique identities and individuality within a free and democratic society. Privacy is the legal umbrella for the 'autonomic capabilities'[730] of individuals, which entails their capacity to control their life and to live freely according to their own wishes and choices. Data protection, on the other hand, involves the right to informational self-determination, which incorporates the right of the individuals to exercise control over their data and any decisions made based on those data. This control is a condition precedent for the individuals to preserve their 'autonomic capabilities' in order to freely shape the narrative structure of their life and live according to their own autonomous choices.

Profiling allows business entities to make decisions on behalf of individuals that concern or affect them without their consent or knowledge. This implies a lack of individuals' capacity to control their data and make their own autonomous decisions and choices in order to control their life. In this way, profiling reduces individuals' capacity to freely shape the narrative structure of their life and to develop their own unique personality and identity in order to participate freely within society. Lewis Mumford, in his theory about democracy, claimed that:

> 'All living organisms are in some degree autonomous, in that they follow a life-pattern of their own; but in man this autonomy is an essential condition for his further development. We surrender some of our autonomy when ill or crippled, but to surrender it everyday on every occasion would be to turn life itself into a chronic illness. The best life possible (…) is one that calls for an ever greater degree of self-direction, self-expression, and self-realization. In this sense,

[730] Rouvroy and Poullet 2009 (n 202) 45.

> personality, once the exclusive attribute of kings, belongs on democratic theory to every man. Life in its fullness and wholeness cannot be delegated'[731]

So viewed, the importance of safeguarding privacy and data protection rights from the use of profiling technologies and the consequential profiling practices does not only lie in the prediction and disclosure of knowledge about individuals' identities and their sensitive information, but also lies in the fact that profiling manages individuals' behaviour, actions, thoughts and feelings in ways that may affect their existence, their development and their effective participation in the democratic process of the society in which they live. Arguably, therefore, profiling may challenge democracy and create potentials for social control and normalisation of the individuals.

In this sense, the collection, processing and combination of individuals' data may pose a threat to the basic fundamental principles of a democratic society as well as to the relationship between controllers and individuals, either as citizens or as customers. The resulting lack of control and the unbalanced distribution of powers may create an environment of a transparent – Panopticon – society under which the legitimate opacity of the individuals to preserve their 'right to be let alone' and to control the narrative structure of their life is challenged against the legitimate interests of the controllers for business and profit.

The main research question of this thesis was the following: *Does the transparent and self-determinatory (controllable) nature of data protection law safeguard the protection of the fundamental rights and freedoms of individuals, especially the rights to privacy and data protection, in today's profiling-based society?*

[731] Lewis Mumford, 'Authoritarian and Democratic Technics' (1964) Technology and Culture 5(1) 1–8.

Following the above analysis, this question can be answer negatively. From the findings revealed in the previous chapters, in terms of profiling, the transparent and self-determinatory (controllable) nature of data protection law is ineffective to provide and ensure protection for individuals and their rights.

The logic and scope behind the adoption of data protection legislation, and thus of the GDPR, is the co-existence of fundamental rights with the Internal Market rules. As such, data protection legislation does not only intend to prevent fundamental rights abuses by market actors, but it also focuses on the development of the common market and free movement regime. For this reason, the default position of data protection legislation is the transparency of the controller. In contrast to opacity rules which prohibit any unlawful and excessive interference in individuals' private lives (except under the conditions provided in Article 8(2) of the ECHR and Article 7(2) of the Charter), the transparency rules are non-prohibitive in nature in the sense that they do not prohibit interference with individuals' data but they control such interference. In other words, the law, on the one hand, regulates the acceptable level for controllers to collect and process individuals' data for profiling while, on the other hand, provides for individuals the means to control such profiling.

Transparency, therefore, and data protection legislation, remain consistent with the idea of informational self-determination which presupposes that individuals should be able to make conscious and autonomous decisions about their data. Such decisions enable individuals to exercise control over their data and thus over their lives in order to maintain their autonomy and individuality within society. However, from the findings revealed in this thesis, control on the part of individuals is inconsistent with profiling. This is because:

Firstly, consent, which supposedly gives individuals the means to control their data and aspects of their identities and personalities within society, and which is the foundational element of the EU data protection legislation to ensure fair and lawful use of the data, does not prove to be an effective mechanism. This is because consent has been proved to be a pseudo-right, under which the individuals do not have the choice to refuse to give their data or to withdraw their consent without being denied

the required service or product. Therefore, individuals, in giving their consent, act mechanically and unconsciously due to the fear of losing the service. Such consent cannot be considered as the freely given, specific, informed and unambiguous indication of the individuals' wishes.

Secondly, the way profiling works interferes with individuals' autonomy and self-determination. Profiling by nature creates knowledge asymmetries which result in the unbalanced distribution of powers between individuals and business entities. This means limited knowledge and lack of awareness on the part of individuals which, undoubtedly, results in limited control over their data. There is also a lack of individuals' capacity to participate in the decision-making process because profiling enables business entities to make decisions on behalf of individuals or to influence individuals to decide in a certain way. In addition, profiling forces people to live according to their pasts by inferring knowledge based on their previous behaviour and choices. The narrative structure of life, however, must enable individuals to change or improve their lives and not to be captivated by their past behaviours. In this way, profiling, by its functioning nature, reduces the capacity of individuals to freely shape the narrative structure of their lives and thus exercise control.

Thirdly, profiling encourages loss of control and separation from the real self. Instead of acting as an individual, a person experiences a lack of self-awareness, loss of individuality and personal responsibility and loss of self-regulation. This means that the person loses his/her identity and personality and becomes vulnerable to external conditions (to the opinions and behaviours of others). More importantly, the lack of self-regulation makes the individual lose control, and any sense of control, over him/herself and thus over his/her life, thoughts, emotions, and actions. Therefore, it is not expected that the controllable and self-determinatory nature of the law effectively protects the individuals, if the individuals themselves have no interest either in exercising such control or to live a self-determined existence (to make their own decisions without interference by others). What is even worse is that the individuals are neither aware nor able to be aware that they are in this situation (lack of knowledge and self-regulation).

One might argue that, since profiling changes individuals and their interests and creates models of new identities and personalities through the process of generalisation and categorisation of behaviour, individuals' sense of control or the way they exercise control may change too. This, however, is not true because: (a) these new models of identity and personality do not constitute the real self of the individual; (b) it is not the individual's free and autonomous choice to change his/her self and create a new personality (thoughts, interests, habits etc.); (c) the individual does not realise that he/she have changed; (d) the individual does not have the ability to realise what is good or bad or what is right and wrong for him/her because he/she has lost his/her real self and thus his/her sensibility and good judgement to make decisions about him/herself as a unique single entity.

Finally, profiling is a Panopticon. A Panopticon is a system of social control and correction of individuals' behaviour in different contexts of life. This means the acceptance and compliance of the individuals with the rules. Individuals held in a Panopticon are directed to adopt disciplined behaviour not only because of the fear of being observed at any time but also because of the further, deeper knowledge and analysis of their lives by the business entities. The idea of a Panopticon, therefore, is to correct and control individuals' behaviour and not to leave them free to exercise, by themselves, control over their own lives by making their own free and autonomous decisions and choices.

To conclude, profiling contradicts the idea of transparency and the self-determinatory nature of data protection legislation and thus of the GDPR. The idea of empowering individuals to protect themselves through the exercise of control (consent mechanism) over their data and of their lives is antithetic to the scope of profiling and essentially to group profiling – generalisation – which is the *new oil* of the profiling-based society. Consequently, in the absence of the exercise of such control, individuals are left powerless against their profilers and their profiling activities towards their data, their privacy and their life.

The problem of profiling is considered as a dispute between data subjects and controllers or dispute between individuals and market actors; as a technological,

business or legal question, while in actual fact it is a pure question of protecting human rights.

It is my opinion, therefore, that the protection of individuals should be left to the legislator to exercise control on the part of the individuals rather than to the individuals themselves. It is also my opinion that profiling constitutes a humanitarian issue which must be embedded in the sphere of humanitarian law. For this reason, there should be a stand-alone law of profiling with a prohibitive – humanitarian – nature, in combination with fundamental human rights-based law.

This means that profiling should be incorporated as an autonomous – prohibitive – fundamental human right in the EU Charter: *'the right not to be subject to profiling and to automated decision-makings'*. The exceptions (transparency rules) provided in such a right should be strict, explicit and limited to certain and precise circumstances, leaving no room for various interpretations or re-profiling. Such a right and such a stand-alone law should protect individuals from group profiling and generalisation, from automated decision-makings, from monitoring and real-time surveillance, from normalisation and social control, from future knowledge which may be revealed from the analysis of the individuals' data as well as ensure the protection of individuals' identities, personalities and individuality. In addition, both the fundamental right and the stand-alone law of profiling should also be consistent with the right to privacy as provided in the ECHR and the EU Charter. For this reason, however, the exceptions provided in Article 8(2) of the ECHR and in Article 7(2) of the EU Charter should be made more strict, prohibitive and precise in order to prevent another general exception of the type of the statistical purpose.

For this reason, it is my suggestion that future research must be conducted to examine: (a) the regulation of profiling within the framework of humanitarian law and the provisions of a stand-alone law of profiling; (b) the incorporation of profiling as an autonomous fundamental right of a prohibitive nature in the Charter; and (c) how the exceptions provided in Article 8(2) of the ECHR and in Article 7(2) of the EU Charter will be transformed in order to be strict, prohibitive and precise.

Bibliography

Primary Sources

International Legislation

European Convention of Human Rights and Fundamental Freedoms 1950: Convention for the Protection of Human Rights and Fundamental Freedoms as amended by Protocols No. 11 and No. 14

International Covenant on Civil and Political Rights 1966 (ICCPR)

Universal Declaration of Human Rights as proclaimed by the General Assembly of the United Nations on 10th December 1948 (UDHR)

EU Legislation

Charter of Fundamental Rights of the European Union as proclaimed by the European Parliament, the Council and the Commission on 18th December 2000, OJ C 83, 30/03/2010 P. 389-403

Convention for the Protection of Individuals Regarding to Automatic Processing of Personal Data, signed in Strasbourg on 28th January 1981 (Convention 108)

Directive 95/46/EU of the European Parliament and of the Council of October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23/11/1995 P. 0031-0050

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31/07/2002 P. 0037-0047

Directive 2000/43/EC of the Council of the European Union of 29 June 2000 implementing the principle of equal treatment between persons irrespective of racial or ethnic origin OJ L 180, 19/07/2000 P. 0022 – 0026

Directive 2004/113/EC of the Council of the European Union of 13 December 2004 implementing the principle of equal treatment between men and women in the access to and supply of goods and services OJ L 373, 21/12/2004 P. 37 – 43

Organisation for Economic Cooperation and Development Guidelines (OECD) Council Recommendations on the Protection of Privacy and Transborder Flows of Personal Data, 23 September 1980

Proposal for a Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data (COM(92) 422

final – SYN 287, 15.10.1992) <http://aei.pitt.edu/10375/1/10375.pdf> (accessed 1 May 2016))

Proposal for a Regulation 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 (General Data Protection Regulation), COM (2012), 25/01/2012

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, and Repealing Directive 95/46/EC (General Data Protection Regulation)

Recommendation CM/Rec(2010)13 and explanatory memorandum on the protection of individuals with regard to automatic processing of personal data in the context of profiling adopted by the Committee of Ministers of the Council of Europe on 23 November 2010

UK Legislation

UK Human Rights Act 2000

Article 29 Working Party Opinions

Article 29 Working Party, 'Opinion No. 8/2014 16 on the Recent Developments on the Internet of Things' adopted on 16th September 2014 (14/EN/WP 223)

Article 29 Working Party, 'Opinion No. 03/2013 on Purpose Limitation' adopted on 2nd April 2013 (00569/13/EN WP 203)

Article 29 Working Party 'Opinion No. 15/2011 on the Definition on Consent', adopted on 13th July 2011 (01197/11/EN, WP 187)

Article 29 Working Party, 'Opinion No. 4/2007 on the Concept of Personal Data', adopted on 20th June 2007 (01248/07/EN, WP 136)

Article 29 Working Party, 'Opinion No. 3/2010 on the Principle of Accountability', adopted on 20th June 2007 (00062/10/EN, WP 173)

Article 29 Working Party, 'Working Document on the Processing of Personal Data Relating to Health in Electronic Health Records (HER)', adopted on 15th February 2007 (00323/07/EN, WP 131)

Article 29 Data Protection Working Party, 'Working Document on Data Protection Issues Related to RFID Technologies', adopted on 19 January 2005 (10107/05/EN, WP 105)

Article 29 Working Party, 'Document on the Blacklist', adopted on 3th October 2002 (11118/02/EN, WP 65)

Case Law

Amann v. Switzerland App no 27798/95 (ECtHR, 16 February 2000), ECHR 2000-II

Hatton v. United Kingdom App no 36022/97 (ECtHR, 8 July 2003), 15 BHRC 259

M.M. v. United Kingdom App no 24029/07 (ECtHR, 13 November 2012)

Niemitz v. Germany App no 13710/88 (ECtHR, 16 December 1992)

Odievre v. France App no 42326/98 (ECtHR, 13 February 2003)

Pretty v. United Kingdom App no 2346/02 (ECtHR, 29 April 2002)

Rotaru v. Romania App no 28341/95 (ECtHR, 5 May 2000)), ECHR 2000-V

Von Hannover v. Germany App no 59320/00 (ECtHR, 24 June 2004)

CJEU 8 April 2014, C-293/12 and C-594/12 (*Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Recourses*)

CJEU 13 May 2014, C-131/12 (*Google Spain v Costeja González*)
CJEU 6 November 2003, C-101 (*Lindqvist*)

CJEU 19 November 1998, C-162/97 (*Nilsson, Hagelgren and Arrborn*)

CJEU 1 October 2015, C-230/14 (*Weltimmo*)

Case T-194/04 *Commission v. Bavarian Lager Co. Ltd* [2007] ECR II – 4532

Association belge des Consommateurs Test-Achats ASBL and Others v Conseil des ministers Case C-236/09

Consent to Advertising by E-Mail and SMS, Re (VIII ZR 348/06) Bundesgerichtshof (Germany) 16 July 2008, [2009] E.C.C. 27

CTN Cash and Carry Ltd. v Gallaher Ltd [1993] EWCA Civ 19

Durant v Financial Services Authority [2003] EWCA Civ 1746

Universe Tankships v International Transport Workers Federation, The Universal Sentinel [1983] 1 AC

Volkszählungsurteil BVerfGE 1, 68-69 (1983)

X v. Iceland App no 6825/74 (Commission decision 18 May 1976)

Secondary Sources

Books

Beale H (ed), *Chitty on Contracts 30th edition* (UK: Sweet & Maxwell Ltd 2008)

Bentham J (ed), *Panopticon; or, The Inspection – House* (Dodo Press 2008)

Candy O (ed), The Panoptic Sort: Political Economy of Personal Information (Critical Studies in Communication and in Culture Industries' (Westview Press: 1993)

Constandinides G, 'The New Encyclopediko Dictionary of the Old Testament' (2nd edn, Publigations The Logos 1985) 201 – 202 (In Greek: Γεώργιου Ζ. Κωνσταντινίδη (Β' Έκδοση), '*ΝΕΟΝ ΕΓΚΥΚΛΟΠΑΙΔΙΚΟΝ ΛΕΞΙΚΟΝ ΑΓΙΑΣ ΓΡΑΦΗΣ*' (Εκδόσεις 'Ο Λόγος' 1985) 201–202)

Cooter R (ed), 'The Cultural Meaning of Popular Science: Phrenology and the Organization of Consent in Nineteenth-Century Britain' (Cambridge: University Press 1984)

Custers B (ed), 'The Power of Knowledge - Ethical. Legal and Technological Aspects of Data Mining and Group Profiling in Epidemiology' (Wolf Legal Publishers 2004)

Duval S and Wicklund R (ed), *A Theory of Objective Self-Awareness* (New York: Academic Press 1972)

Ferretti F (ed), *EU Competition Law, the Consumer Interest and Data Protection: The Exchange of Consumer Information in the Retail Financial Sector* (Springer 2014)

Fischer J (ed), *Free Will, Death and Immorality: The Role of Narrative* (New York: Oxford University Press 2009)

Forsythe D (ed), *Human Rights in International Relations* (Cambridge University Press 2000)

Foucault M (ed), *Discipline and Punish: The Birth of the Prison* (New York: Vintage Books 1977)

Craig P and De Burca G, *EU Law: Text, Cases, and Materials* (2nd edn, Oxford University Press 1998)

Guest A G, *Chitty on Contracts 27th edition* (UK: Sweet & Maxwell Ltd 1994)

Guest A G, *Chitty on Contracts 25th edition* (UK: Sweet & Maxwell Ltd 1983)

Hijmans H and Kranenborg H (ed), *Data Protection Anno 2014: How to Restore Trust? Peter Hustinx, European Data Protection Supervisor (2004-2014)* (Cambridge: Intersentia Publishing Ltd. 2014)

Hildebrandt M and Gutwirth S (ed), *Profiling the European Citizen: Cross-Disciplinary Perspectives* (Springer Science + Business Media 2008)

Lloyd I, *Information Technology Law* (6th edn, OUP 2011)

O'Hara K and Shadbolt N (ed), *The Spy In The Coffee Machine. The End of Privacy As We Know It* (Oneworld Publications 2008)

Roosendaal A (ed), *Digital Personae and Profiles in Law: Protecting Individuals' Rights in Online Contexts* (Wolf Legal Publishers 2013)

Sampson E E and Marthas M S (ed), *Group Process for the Health Professions* (New York: John Wiley & Sons Inc 1981)

Savin A (ed), *EU Internet Law* (Edward Elgar Publishing Ltd. 2013)

Smith A S (ed), *Contract Theory* (Oxford University Press 2004) 331-33

Solove D (ed), *Understanding Privacy* (HUP 2008)

Solove D (ed), *The Digital Person: Technology and Privacy in the Information Age* (New York University Press 2004)

'The Old Testament' in Today's Greek Version (Greek Publications 1997) 220 – 221 (In Greek: 'Η ΠΑΛΑΙΑ ΔΙΑΘΗΚΗ' (Έκδοση Ελληνικής Βιβλικής Εταιρείας 1997) 220 – 221)

Mavrias C, '*Constitutional Law*' (3rd edn, Athens: Sakkoula Publications 2004) 137 – 142) (In Greek: Κώστας Γ. Μαυριάς (Τρίτη Έκδοση), *'Συνταγματικό Δίκαιο'* (Εκδόσεις Αντ. Ν. Σάκκουλα 2004) 137 – 142)

Ofstad H (ed), *An Inquiry into the Freedom of the Decision* (Norwegian University Press 1961)

Contributions to Edited Books

Agre PE, 'Introduction' in Agre PE and Rotenberg M (eds), *Technology and Privacy: The New Landscape* (MIT Press1997)

Andrade N, 'Data Protection, Privacy and Identity: Distinguishing Concepts and Articulating Rights' in Fischer-Hübner et al. (eds), Privacy and Identity Management for Life. Privacy and Identity 2010 IFIP Advances in Information and Communication Technology, vol 352. (Springer, Berlin, Heidelberg 2011)

Benoist E, 'Collecting Data for the Profiling of Web Users' in Hildebrandt M and Gutwirth S (eds), *Profiling the European Citizen: Cross-Disciplinary Perspectives* (Springer 2008)

Berlin I, 'Two Concepts of Liberty' (1958) in Berlin I (ed), *Four Essays on Liberty* (Oxford University Press 1969)

Bieruat M and Boridio J, 'Stigma and Stereotypes' in Heatherton T F et al. (eds), *The Social Psychology of Stigma* (The Guilford Press 2003)

Bosco F et al., 'Profiling Technologies and Fundamental Rights. An Introduction' in Creemers N, Guagninn D and Koops B (eds), *Profiling Technologies I Practice: Applications and Impact on Fundamental Rights and Values* (Wolf Legal Publishers 2015)

Bosco F et al., 'National Data Protection Authorities' views on Profiling' in Creemers N et al. (eds), *Profiling Technologies in Practice: Applications and Impact on Fundamental Rights and Values* (Wolf Legal Publishers 2015)

Canhoto A and Backhouse J, 'General Description of the Process of Behavioural Profiling' in Hildebrandt M and Gutwirth S (eds), *Profiling the European Citizen: Cross-Disciplinary Perspectives* (Springer 2008)

Crocker J, Major B and Steele C, 'Social Stigma' in Gilbert D, Fiske S and Lindzey G, *The Handbook of Social Psychology* (4th edn, OUP 1998)

Custers B, 'Effects of Unreliable Group Profiling by Means of Data Mining' in Grieser G, Tanaka Y and Yamamoto A (eds), *Discovery Science*: *6th International Conference, DS 2003, Sapporo, Japan, October 17-19, 2003. Proceedings* (Springer 2003)

Custers B, 'Data Dilemmas in the Information Society: Introduction and Overview' in Custers B et al. (eds), *Discrimination and Privacy in the Information Society (Springer, Berlin, Heidelberg* 2013)

De Hert P and Gutwirth S, 'Privacy, Data Protection and Law Enforcement: Opacity of the Individual and Transparency of the Power' in Claes E, Duff A and Gutwirth S (eds), *Privacy and The Criminal Law* (Intersentia 2006)

De Hof S and Corien Prins C, 'Personalization and Its Influence on Identities, Behaviour and Social Values' in Hildebrandt M and Gutwirth S (eds), *Profiling the European Citizen: Cross-Disciplinary Perspectives* (Springer 2008) 121

Diener E, 'Deindividuation: The Absence of Self-Awareness and Self-Regulation in Group Members' in Paulus P (eds), *The Psychology of Group Influence* (Lawrence Erlbaum 1980)

Dinant J-M, 'The Concepts of Identity and Identifiability: Legal and Technical Deadlocks for Protecting Human Beings in the Information Society?' in Gutwirth S et al. (eds), *Reinventing Data Protection?* (Springer Science + Business Media 2009)

Finn R, Wright D and Friedewald M, 'Seven Types of Privacy' in Gutwirth S et al. (eds), *European Data Protection: Coming of Age* (Springer Science+Business Media 2013)

Fritsch L, 'Profiling and Location-Based Services (LBS)' in Hildebrandt M and Gutwirth S (eds), *Profiling the European Citizen: Cross-Disciplinary Perspectives* (Springer 2008) 147

Gutwirth S and de Hert P, 'Regulating Profiling in a Democratic Constitutional State' in Hildebrandt M and Gutwirth S (eds), *Profiling the European Citizen: Cross-Disciplinary Perspectives* (Springer Science+Business Media 2008)

Gutwirth S and Hildebrandt M, 'Some Caveats on Profiling' in Gutwirth S, Pullet Y and de Hert P (eds), *Data Protection in a Profiled World* (Springer 2010)

Hildebrandt M, 'Defining Profiling: A New Type of Knowledge?' in Hildebrandt M and Gutwirth S (eds), *Profiling the European Citizen: Cross-Disciplinary Perspectives* (Springer 2008)

Hildebrandt M, 'Profiles and Correlatable Humans' in Stehr N and Weiler B (eds), *Who Owns Knowledge?* (Transaction Publishers 2006)

Hildebrandt M, 'Profiling and the Identity of the European Citizens' in Hildebrandt M and Gutwirth S (eds), *Profiling the European Citizen: Cross-Disciplinary Perspectives* (Springer Science+Business Media 2008)

Hildebrandt M, 'Technology and the End of Law' in (2009) in Keirsbilck B, Devroe W and Claes E (eds), *Facing the Limits of the Law* (Springer 2009)

Hildebrandt M, 'Who is Profiling Who? Invisible Visibility' in Gutwirth S et al. (eds), *Reinventing Data Protection?* (Springer 2009)

Kamiran F and Žliobaitė I, 'Explainable and Non-explainable Discrimination in Classification' in Custerset B et al. (eds), *Discrimination and Privacy in the Information Society: Data Mining in Large Databases* (Springer 2013)

Kamp M, Korffer B and Meints M, 'Profiling of Customers and Consumers – Customer Loyalty Programmes and Scoring Practices' in Hildebrandt M and Gutwirth S (eds), *Profiling the European Citizen: Cross-Disciplinary Perspectives* (Springer Science+Business Media 2008)

Kohnstamm J, 'Privacy By Debate: The European Data Protection Supervisor's Contribution to Collaboration Between National Data Protection Authorities' in Hijmans H and Kranenborg H (eds), *Data Protection Anno 2014: How to Restore Trust? Peter Hustinx, European Data Protection Supervisor (2004–2014)* (Cambridge: Intersentia Publishing Ltd. 2014)

Leenes R, 'Regulating Profiling in a Democratic Constitutional State. Reply: Addressing the Obscurity of Data Clouds' in Hildebrandt M and Gutwirth S (eds.), *Profiling the European Citizen: Cross-Disciplinary Perspectives* (Springer 2008)

Lyon D, 'Introduction' in Lyon D (ed), *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination* (Routledge Publishing 2003)

Lyon D, 'Surveillance as Social Sorting: Computer Codes and Mobile Bodies in Lyon D (ed), *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination* (Routledge Publishing 2003)

Marchand R, 'Customer Research as Public Relations: General Motors in the 1930' in Strasser S et al. (eds), *Getting and Spending European and American Consumer Societies in the Twentieth Century* (Washington D.C. Cambridge University Press 1998)

Mobasher B, 'Data Mining for Web Personalization' in Brusilovsky P, Kobsa A and Nejdl W (eds), *The Adaptive Web: Methods and Strategies of Web Personalization* (Springer 2007)

Norris C, 'From Personal to Digital: CCTV, the Panopticon, and the Technological Mediation of Suspicion and Social Control' in Lyon D (eds), *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination* (Routledge Publishing 2003)

Onut S, Erdem I and Hosver B, 'Customer Relationship Management in Banking Sector and A Model Design for Banking Performance Enhancement' in Minai A and Bar-Yam Y (eds), *Unifying Themes in Complex Systems IV: Proceedings of the Fourth International Conference on Complex Systems* (Springer 2008)

Phillips D and Curry M, 'Privacy and the Phenetic Urge: Geodemographics and the Changing Spatiality of Local Practice' in Lyon D (eds), *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination* (Routledge Publishing 2003)

Poullet Y, 'About the E-Privacy Directive: Towards a Third Generation of Data Protection Legislation? in Gutwirth S, Poullet Y and de Hert P (eds), *Data Protection in a Profiled World* (Springer 2010)

Prins C, 'Averse from Hair-splitting: A Process-based Framework to Balance Privacy and Other Interests' in Hijmans H and Kranenborg H (eds), *Data Protection Anno 2014: How to Restore Trust? Peter Hustinx, European Data Protection Supervisor (2004–2014)* (Cambridge: Intersentia Publishing Ltd. 2014)

Rouvroy A and Poullet Y, 'The Right to Informational Self-Determination and the Value of Self-Determination: Reassessing the Importance of Privacy for Democracy' in Gutwirth S et al. (eds), *Reinventing Data Protection?* (Springer 2009)

Sartor G, 'Privacy, Reputation, and Trust: Some Implications for Data protection' in Stolen et al. (eds), *Trust Management* (Springer 2006)

Schermer B W, 'Risks of Profiling and the Limits of Data Protection Law' in Custers B et al. (eds), *Discrimination and Privacy in the Information Society: Data Mining in Large Databases* (Springer 2013)

Schreurs W et al., 'Cogitas, Ergo Sum. The Role of data protection and Non-Discrimination Law in Group Profiling in the Private Sector' in Hildebrandt M and

Gutwirth S (eds), *Profiling the European Citizen: Cross-Disciplinary Perspectives* (Springer 2008)

Thomas R, 'Accountability – A Modern Approach to Regulating the 21st Century Data Environment' in Hijmans H and Kranenborg H (eds), *Data Protection Anno 2014: How to Restore Trust? Peter Hustinx, European Data Protection Supervisor (2004–2014)* (Cambridge: Intersentia Publishing Ltd. 2014)

Walden I, 'Privacy and Data Protection' in Reed C, *Computer Law* (7th edn, OUP 2011)

Yannopoulos A, Andronikou V and Varvarigou T, 'Behavioural Biometric Profiling' in Hildebrandt M and Gutwirth S (eds), *Profiling the European Citizen: Cross-Disciplinary Perspectives* (Springer 2008)

Yannopoulos A, Andronikou V and Varvarigou T, 'Biometric Profiling: Opportunities and Risks' in Hildebrandt M and Gutwirth S (eds), *Profiling the European Citizen: Cross-Disciplinary Perspectives* (Springer 2008)

Journal Articles

Acquisti A and Varian H, 'Conditioning Prices on Purchase History' (2005) 24(3) *Marketing Science* 367

Acquisti A, 'Identity Management and Price Discrimination' (2008) 6(2) *IEEE Security & Society* (March/April) 47

Altshuler R, 'Free Will, Narrative, and Retroactive Self-Constitution' (2014) *Phenomenology and the Cognitive Sciences* (ISSN: 1568-7759 (print) 1572-8676 (online)) 1

Bergelson V, 'It's Personal but Is It Mine? Towards Property Rights in Personal Information' (2003) 37(2) *University of California, Davis Law Review* 379

Bignami F, 'Privacy and Law Enforcement in the European Union: The Data Retention Directive' (2007) *Chicago Journal of International La*w 8(1) 235

Blume P, 'Symposium on EU Data Protection Reform: The Myths Pertaining to the Proposed General Data Protection Regulation' (2014) *International Data Privacy Law* 1

Borgesius Z F, 'Behavioral Targeting: A European Legal Perspective' (2013) *IEEE Security & Privacy* 11(1) 82

Borghi M, Ferretti F and Karapapa S, 'Online Data Processing Consent under EU Law: A Theoretical Framework and Empirical Evidence from the UK' (2013) 21(2) *International Journal of Law and Information Technology* 109

Brody R, 'Consequences of Electronic Profiling' (1999) 18(1) *IEEE Technology and Society Magazine* 20

Bygrave L, 'Automated Profiling – Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling' (2001) 17(1) *Computer Law & Security Report* 17

Bygrave L, 'The Place of Privacy in Data Protection Law' (2001) 24(1) *UNSW Law Journal* 277

Bygrave L, 'Data Protection Law; Approaching Its Rationale, Logic and Limits' (2002) 10 *Information Law Series* (The Hague/London/New York: Kluwer Law International) 291

Chalton S, 'Reflections on *Durant v FSA*' (2004) 20(3) *Computer Law & Security Report* 175

Chua, B. et al., 'Impacts of cruise service quality and price on vacationers' cruise experience: Moderating role of price sensitivity' (2015) *International Journal of Hospitality Management* 44 131-145

Clarke R, 'Profiling: A Hidden Challenge to the Regulation of data surveillance' (1993) 4(2) *Journal of Law, Information and Science* 403

Clarke R, 'A Normative Regulatory Framework for Computer Matching' (1995) 13(4) *Journal of Computer & Information Law* 585

Costa L and Poulet Y, 'Privacy and the Regulation of 2012' (2012) *Computer Law & Security Review* (3) 255

Couldwell C, 'A Data Day Battle' *Computing* (1998) 64

Crockers J and Major B, 'Social Stigma and Self-Esteem: The Self-Protective Properties of Stigma' (1989) *Psychological Review* 96(4) 60

Culnan M, '"How Did They Get My Name?": An Exploratory Investigation of Consumer Attitudes Towards Secondary Information Use' (1993) 17(3) *MIS Quarterly* 341

Culnan M and Armstrong P, 'Information Privacy Concerns, Procedures Fairness, and Impersonal Trust: An Empirical Investigation' (1999) 10(1) *Organization Science* 104

Curren L and Kaye J, 'Revoking Consent: A 'blind spot' in Data Protection Law?' (2010) 26 *Computer Law & Security Review* 273

Ellwood C A, 'Lombroso's Theory of Crime' (1912) 2(5) *Journal of Criminal Law and Criminology* 716

Epstein R, 'Direct Democracy: Government of the People, by the People, and for the People' (2011) 34 *Harvard Journal of Law and Public Policy* 819

Evans AC, 'European Data Protection Law' (1981) 29 *American Journal of Comparative Law* 571

Fayyad U, 'Data Mining and Knowledge Discovery: Making Sense Out of Data' (1996) 11(5) IEEE Expert 21

Ferretti F, 'The Credit Scoring Pandemic and the European Vaccine: Making Sense of EU Data Protection Legislation' (2009) 1 *Journal of Information, Law & Technology*

Ford R, 'Save the Robots: Cyber Profiling and Your So-Called Life' (2000) 52(5) *Stanford Law Review* 1573

Funsten D, 'Helping Your Customers Behave Themselves' (1998) 30(10) *Bank Marketing* 22

Gary M and Reichman N, 'Routinizing the Discovery of Secrets: Computers as Informants' (1984) 27(4) *American Behavioral Scientists* 423

Gavison R E, 'Privacy and the Limits of Law' (1980) *Yale Law Journal* 89(3) 421–471

Gonzales A and Hancock J, 'Mirror, Mirror on my Facebook Wall: Effects of Exposure to Facebook on Self-Esteem' (2010) 14(1-2) *Cyberpsychology, Behavior, and Social Networking* 79

Gunasekara G, 'Paddling in Unison or Just Paddling? International Trends in Reforming Information Privacy Law' (2013) 22(2) *International Journal of Law and Information Technology* 141

Gutwirth S, 'Biometrics Between Opacity and Transparency' (2007) 43(1) *Annali dell'Istituto Superiore di Sanità* 61

Hacking I, 'Making Up People' (2006) *London Review of Books* 28(16) 23

Hajian S and Domingo-Ferrer J, 'A Methology for Direct and Indirect Discrimination Prevention in Data Mining' (2013) *IEEE Transactions on Knowledge and Data Engineering* 25(7) 1445

Hatch M, 'The Privatization of Big Brother: Protecting Sensitive Personal Information from Commercial Interests in the 21st Century' (2001) 27 *William Mitchell Law Review* 27(3) 1457

Hildebrandt M, 'Profiling: From Data to Knowledge' (2006) 30(9) *Datenschutz und Datensicherheit (DuD)* 548

Hildebrandt M, 'Profiling and the Rule of Law' (2008) 1(1) *Identity in the Information Society (IDIS)* 55

King N and Jessen P W, 'Profiling the Mobile Customer – Privacy when Behavioural Advertisers Target Mobile Phones – Part I' (2010) 26 *Computer Law & Security Review* 455

Klimas T and Vaičiukaitė J, 'The Law of Recitals in European Community Legislation' (2008) ILSA Journal of International & Comparative Law (1) 92

Koops B-J, The Trouble with European Data Protection Law (2014) *International Data Privacy Law* (doi: 10.1093/idpl/ipu023)

Korff D, 'Comparative Summary of National Laws', *EC Study on Implementation of Data Protection Directive* (Study Contract ETD/2001/B5 3001/A/49) 27

Kotschy W, 'The Proposal for a New General Data Protection Regulation – Problem Solved?' (2014) *International Data Privacy Law* 4(4) 274

Kuner C, 'The European Commission's Proposal Data Protection Regulation: A Copernican Revolution in European Data Protection Law' (2012) *Bloomberg BNA Privacy and Security Law Report* 1

Kuner C et al., 'Face-to-data – Another Developing Privacy Threat?' (2013) 3(1) *International Data Privacy Law* 1

Kuner C, Burton C and Pateraki A, 'The Proposed EU Data Protection Regulation Two Years Later' (2014) *BNR Privacy & Security Law Report* 6

Leader S, 'Inflating Consent, Inflating Function, and Inserting Human Rights' in Dine J and Fagan A (eds) *Human Rights and Capitalism* (Edward Elgar 2006) 28–47

Leenes R, 'Do They Know Me? Deconstructing Identifiability' (2007) 4(1-2) *University of Ottawa Law & Technology Journal (UOLTJ)* 135

Marx G, 'What's in a Name? Some Reflections in the Sociology of Anatomy' (1999) 15(2) *Information Society: An International Journal* 99

Marx G, 'What's New About the "New Surveillance"? Classifying for Change and Continuity' (2002) 1(1) *Surveillance & Society* 9

Mayer-Schonberger V and Padova Y, 'Regime Change? Enabling Big Data Through Europe's New Data Protection Regulation' (2016) XVII *The Columbia Science and Technology Law Review* 319

McKenna K and Bargh J, 'Plan 9 From Cyberspace: The Implications of the Internet for Personality and Social Psychology' (2000) *Personality and Social Psychology Review* 4(1) 61

Mumford L, 'Authoritarian and Democratic Technics' (1964) *Technology and Culture* 5(1) 1

Nadler A, Goldberg M and Jaffe Y, 'Effects of Self-differentiation and Anonymity in Group on Deindividuation' (1982) *Journal of Personality and Social Psychology* 42 1127

Parker R, 'A Definition of Privacy' (1974) 27 *Rutgers Law Review* 275

Patrick T, 'Online Profiling' (2000) 34(38) *Computerworld* 56

Reding V, 'The European Data Protection Framework for the Twenty-First Century' (2012) 2(3) *International Data Privacy Law* 119

Rouvroy A, 'Privacy, Data Protection, and the Unprecedented Challenges of Ambient Intelligence' (2008) 2(1) *Studies in Ethics, Law, and Technology* <http://ssrn.com/abstract=1013984>

Ruggieri S, Pedreschi D and Turini F 'Data Mining for Discriminatory Discovery' (2010) 4(2) *ACM Transactions on Knowledge Discovery from Data* Article 9

Schermer B, 'The Limits of Privacy in Automated Profiling and Data Mining' (2011) 27 *Computer Law & Security Review* 45

Schmeiser H, Störmer T and Wagner J, 'Unisex Insurance Pricing: Consumers' Perception and Market Implications' (2016) in *The Geneva Papers*, Palgrave Macmillan, London

Spiecker genannt Döhmann I et al., 'The Regulation of Commercial Profiling – A Comparative Analysis' (2016) *European Data Protection Law Review* 2(4) 535-554

Steinbock D J, 'Data Matching, Data Mining and Due Process' (2005) *Georgia Law Review* 10-18

Stevens L, 'IT Sharpens Data Mining's Focus – Instead of Building data-Mining Application with No Clear Goal. Companies are Setting Priorities Up Front to Maximize ROY' (6 August 2001) *Internet Week* 29

Tzanou M, 'Data Protection as a Fundamental Right Next to Privacy? 'Reconstructing' a Not So New Right' (2013) 3(2) *International Data Privacy Law* 88

Vedder A, 'KDD: The Challenge to Individualism' (1999) 1 *Ethics and Information Technology* 275

Warren S and Brandeis L, 'The Right to Privacy' (1890) 4 *Harvard Law Review* 193

Wahlstrom K, 'On the Ethical and Legal Implications of Data Mining' (2006) *Technical Report SIE-06-001* (School of Informatics and Engineering, Flinders University Adelaide, Australia)

Webber R, 'The Evolution of Direct, Data and Digital Marketing' (2013) 14(4) *Journal of Direct, Data and Digital Marketing Practices* 291–309

Weizer M, 'The Computer of the 21st Century' (September 1991) *Scientific American* 94–104

Woodworth M and Porter S, 'Historical Foundations and Current Applications of Criminal Profiling in Violent Crime Investigations' (1999) 7(4) *Expert Evidence* 24

Yu S, 'Behavioral Evidence Analysis on Facebook: A Test of Cyber-Profiling' (2013) 33 *Defendology Journal* 19

Zarsky T, '"Mine Your Own Business!": Making the Case for the Implications of the Data Mining of Personal Information in the Forum of Public Opinion' (2002–2003) 5(1) *Yale Journal of Law & Technology*

Zarsky T, 'Desperately Seeking Solutions: Using Implementation-Based Solutions for the Troubles of Information Privacy in the Age of Data Mining and the Internet Society' (2004) 56(1) *Maine Law Review* 13

Žliobaitė I, Kamiran F and Calders T, 'Handling Conditional Discrimination' (2011) ICDM '11: Proceedings of the 2011 *IEEE 11th International Conference on Data Mining* 992

Papers and Law Reports

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: 'Safeguarding Privacy in a Connected World – A European Data Protection Framework for the 21st century', COM (2012) 9 final, 25/01/2012

Division of Financial Practices, Bureau of Consumer Protection, 'Privacy Online: Fair Information Practices in the Electronic Market Place. A Report to Congress' (2000) <https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000text.pdf> (accessed 10 June 2018).

Electronic Privacy Information Center and Privacy International, 'Privacy and Human Rights – An International Survey of Privacy Laws and Developments' (2002) (Washington D.C. and London)

Ferraris V et al., 'Defining Profiling' (2013) EU Profiling Project Working Paper <http://profiling-project.eu/wp-content/uploads/2013/07/PROFILINGproject_WS1_definition_2607.pdf> (accessed 13 May 2014).

Ferraris V, Bosco F and E. D'Angelo, 'The Impact of Profiling on Fundamental Rights' (2013) EU Profiling Project Working Paper <http://www.unicri.it/special_topics/citizen_profiling/PROFILINGproject_WS1_Fundamental_1110.pdf> (accessed 13 May 2014).

Hustinx P, 'EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation' (1–12 July 2013) Collected Courses of the European University Institute's Academy of European Law, 24th Session on European Union Law <https://secure.edps.europa.eu/EDPSWEB/edps/EDPS/Publications/SpeechArticle/SA2014> (accessed 05 October 2015).

Information Commissioner's Office (ICO), 'Big Data and Data Protection 20140728 version: 1.0' (2014) <https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2016/11/big-data-and-data-protection.pdf> (accessed 1 July 2018).

Reding V, 'The EU Data Protection Regulation: Promoting Technological Innovation and Safeguarding Citizens' Rights' European Commission (SPEECH/14/175, 4 March 2014) <http://europa.eu/rapid/press-release_SPEECH-14-175_en.htm?locale=en> (accessed 20 April 2016).

U.S. Information Infrastructure Task Force (IITF), 'Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information' (1995) Washington, DC: Department of Commerce).

Online Journals

Custers B et al., 'Informed Consent in Social Media Use – The Gap Between User Expectations and EU personal Data Protection Law' (2013) 10(4) *Scripted (A Journal of Law, Technology and Society)* 435.

Edwards L, 'Big Banker is Watching: In the Brave New Banking World, "Unprofitable" Customers Will Find that Bankers Don't Want them – or Their Money' (22 January 1999) *Bankrate.com* <http://www.bankrate.com/brm/news/bank/19990122.asp> (accessed 9 November 2015).

Hornung G, 'A General Data Protection Regulation for Europe? Light and Shade in the Commission's Draft of 25 January 2012' 9(1) *Scripted (A Journal of Law, Technology and Society)* 64.

Online Newspapers, Magazines, Websites and Blogs

Beal V, 'Big Data' (16 June 2015) <http://www.webopedia.com/TERM/B/big_data.html> (accessed 1 June 2018).

Butler B, 'When does 'big data' become big? AWS, IBM and Research Firms Each Have Their Own Definitions' (2012) NetworkWorld <http://www.networkworld.com/article/2188435/data-center/defining--big-data--depends-on-who-s-doing-the-defining.html> (accessed 2 July 2014).

CCHR Institutions Series, Separation of Powers and the Rule of Law (June 2011) <http://www.a4id.org/sites/default/files/user/Institutions_Fact_Sheet_1_Separation_of_Power.pdf> (accessed 18 August 2015).

Cincotta H, 'Democracy in Brief' (2007) Washington: U.S. Department of State, Bureau of International Information Programs <http://photos.state.gov/libraries/korea/49271/dwoa_122709/Democracy-in-Brief_kor.pdf> (accessed 10 August 2015).

Clarke R, 'What's "Privacy"?' (Version of 7 August 2006) <http://www.rogerclarke.com/DV/Privacy.html> (accessed 10 July 2015).

ComputerWorld.com, <http://www.computerworld.com/article/2983633/microsoft-windows/microsoft-pushes-windows-10-upgrade-to-pcs-without-user-consent.html> (accessed 14 January 2017).

Cowie T, 'Beneficiaries Fear Profiling Stigma' (19 June 2015) <http://www.radionz.co.nz/national/programmes/insight/audio/201758628/insight-for-21-june-2015-child-abuse-or-big-brother> (accessed 8 September 2015).

Custers B, 'Predicting Data that People Refuse to Disclose: How Data Mining Predictions Challenge Informational Self-Determination' (2012) Privacy Observatory Magazine <http://www.privacyobservatory.org/> (accessed 12 November 2015).

Custers B, 'D7.16: Profiling in Financial Institutions' (FIDIS 29 June 2009) FIDIS consortium <http://www.fidis.net/> (accessed 14 July 2014)

Cuthbertson A, 'Is Your Sex Toy Spying on You?' (8 November 2016) Newsweek <https://www.newsweek.com/your-sex-toy-spying-you-489328> (accessed 15 January 2017)

De Pass D, 'Wells Fargo Pulls Criticized Data; Housing Information on Company's Web site is Labelled Racist (BUSINESS)' Star Tribune (Minneapolis,MN) (23 June 2000) <https://www.highbeam.com/doc/1G1-63044933.html> (accessed 13 December 2015)

Duhigg C, 'How Companies Learn Your Secrets' (16 February 2012) New York Times <https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html> (accessed 10 October 2016).

Emmons A, 'Microsoft Pitches Technology That Can Read Facial Expressions at Political Rallies' (2016) <https://theintercept.com/2016/08/04/microsoft-pitches-technology-that-can-read-facial-expressions-at-political-rallies/> (accessed 18 August 2016).

Freberg L (Professor of Psychology at California Polytechnic State University), 'What is De-individualisation?' <http://psych.answers.com/social-psychology/what-is-deindividuation> (accessed 25 April 2015).

Friedland G and Sommer R, 'Cybercasing the Joint: On the Privacy Implications of Geo-Tagging' (2010) International Computer Science Institute <http://www.icsi.berkeley.edu/pubs/techreports/TR-10-005.pdf> (accessed 5 October 2015).

Google Privacy Policy <https://www.google.com/policies/privacy/> (accessed 8 January 2017).

Gutwirth S and de Hert P, 'D7.4: Implications of Profiling Practices in Democracy' (FIDIS 05 September 2005) FIDIS consortium <http://www.fidis.net/resources/fidis-deliverables/profiling/#c1762> (accessed 15 July 2015).

Harris Poll 1998 on Privacy <http://www.businessweek.com/1998/11/b3569104.htm> (accessed 10 June 2016).

Hildebrandt M and Backhouse J, 'D 7.2: Descriptive Analysis and Inventor of Profiling Practices' (2005) FIDIS consortium <http://www.fidis.net/resources/deliverables/profiling/> (accessed 14 July 2014).

Hildebrandt M, Gutwirth S and De Hert P, 'D7.4: Implications of Profiling Practices in Democracy' (FIDIS 05 September 2005) FIDIS consortium <http://www.fidis.net/> (accessed 15 July 2015).

Janik E, 'The Shape of Your Head and the Shape of Your Mind' (6 January 2014) <https://www.theatlantic.com/health/archive/2014/01/the-shape-of-your-head-and-the-shape-of-your-mind/282578/> (accessed 22 September 2017).

Marx G, 'Privacy and Technology' (September 1990) The World and I <http://www.worldandi.com/> (accessed 10 July 2015).

Mont M C et al., 'On the Management of Consent and Revocation in Enterprises: Setting the Context' (2009) HPL-2009-49 HP Laboratories Technical Reports <https://pdfs.semanticscholar.org/7ec6/0b7f34497dc170e8a4d85ac30263dbe2f697.pdf> (accessed 17 January 2017).

Penenberg A, 'The End of Privacy' (1999) <http://www.forbes.com/forbes/1999/1129/6413182a.html> (accessed 19 November 2015).

Pasquale F, 'Op-Ed: We're Being Stigmatized by 'big data' Scores We don't Even Know About' (15 January 2015) Los Angeles Times <http://www.latimes.com/opinion/op-ed/la-oe-0116-pasquale-reputation-repair-digital-history-20150116-story.html> (accessed 8 September 2015).

Peterson S, <http://www.huffingtonpost.com/steve-peterson/warning-your-computer-may_b_10099208.html> (accessed 8 August 2018)

Pfitzmann A and Hansen M, 'Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management: A Consolidated Proposal

for Terminology' (2008) <https://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.31.pdf> (accessed 21 April 2015).

Reidy D, '"Stigma in Social Death": Mental Health Consumer/Survivors Talk About Stigma in their Lives' (Education for Community Initiatives Holyoke, MA 1993) <http://akmhcweb.org/articles/StigmaisSocialDeath.htm> (accessed 8 September 2015).

Schreurs W et al., 'Report on actual and possible profiling techniques in the field of ambient intelligence, FIDIS (Future of Identity in the Information Society)' (2005) FIDIS Deliverable D7.3 <http://www.fidis.net> (accessed 3 July 2018).

Schultz A M, 'History and Effects of Witchcraft Prejudice and Intolerance on Early Modern Women' (5 April 2017) <https://exemplore.com/wicca-witchcraft/Gender-Bias-in-Witch-hunts> (accessed 25 September 2017).

Sunstein C, 'The Daily We: Is the Internet Really a Blessing for Democracy?' (2001) Boston Review <http://bostonreview.net/cass-sunstein-internet-democracy-daily-we> (accessed 10 January 2015).

Vermeulen M, 'Regulating Profiling in the European Data Protection Regulation – An interim insight into the drafting of Article 20' (2013) <http://emsoc.be/wp-content/uploads/2013/11/D3.2.2-Vermeulen-Emsoc-deliverable-profiling-Formatted1.pdf> (accessed 13 May 2014).

Online Dictionaries

Dictionary.com, <http://www.dictionary.com/browse/statistical> (accessed 27 November 2016).

Oxford Dictionary, <https://en.oxforddictionaries.com/definition/profiling> (accessed 2 March 2018).

The Free Dictionary, <http://www.thefreedictionary.com/deindividuation> (accessed 25 April 2015).

WordSense.eu Dictionary, <http://www.wordsense.eu/privatus/> (accessed 8 August 2015).