8 JUNE 2018

GDPR & CONVENTION 108: ADEQUATE PROTECTION IN A BIG DATA ERA?

MARGOT LENS - 2005419
TILBURG UNIVERSITY – LLM LAW AND TECHNOLOGY
Supervisor 1: R.MR. Gellert, Supervisor 2: K.K. E Silva
Word count: 15.503

Table of Content

Chapter 1 – Introduction

1.1 Background

In today's technological environment, personal data is being collected everywhere, by everyone. By the government (e.g. through monitoring the public space with CCTV), by companies (e.g. by tracking cookies), by your fellow citizens (e.g. through the use of their smartphones).[1] Especially with the emergence of Big Data, governments and businesses are able to collect and process large amounts of data. Big Data can be gathered from various sources such as data gathered online through the use of Facebook, but also through the Internet of Things and cloud computing.[2] These Big Data can be used for profiling, which is used for various purposes ranging from anti-terrorism to direct marketing.[3] On the one hand businesses, governments and even consumers can profit from the practice of profiling. On the other hand, the mere existent of profiling, together with the abuse or misuse thereof could have severe consequences for individuals and society. Especially with regard to their fundamental rights and freedom.[4]

Already in the 1960s, governments and businesses were able to set up extensive data banks, and thus improve and increase the collection, processing, and interlinking of personal data.[5] In the light of the aforementioned concerns, the Council of Europe (CoE) decided to establish a framework of norms and principles governing the unfair collection and processing of personal data. In 1981, the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) was concluded.[6] Convention 108 was the first legally binding international instrument in the data protection field. The purpose of the Convention is to secure the rights and fundamental freedoms of individuals, in particular, the right to privacy, with regard to automatic processing of personal data.[7] Under the Convention, the parties are required to take the necessary steps to implement the provisions in their national legislation.

In the 1990s, the need for harmonization of data protection legislation led to an EU-level initiative. Which resulted in the adoption of the European Commission's Data Protection

---

[1] Bart van der Sloot, 'A New Approach to the Right to Privacy, or How the European Court of Human Rights Embraced the Non-Domination Principle' [2017] Computer Law & Security Review <http://linkinghub.elsevier.com/retrieve/pii/S0267364917303849> accessed 5 April 2018.

[2] Henry Pearce, 'Big Data and the Reform of the European Data Protection Framework: An Overview of Potential Concerns Associated with Proposals for Risk Management-Based Approaches to the Concept of Personal Data' (2017) 26 Information and Communications Technology Law 312.

[3] Bart W Schermer, 'The Limits of Privacy in Automated Profiling and Data Mining' (2011) 27 Computer Law and Security Review 45.

[4] ibid.

[5] Council of Europe, Convention 108 and Protocol: background. Available online: <www.coe.int/en/web/data-protection/background>.

[6] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (adopted 28 January 1981, entered into force 1 October 1985), ETS No. 108 (Convention 108).

[7] ibid., Article 1.

Directive (DPD) in 1995.[8] The Directive regulates the protection of individuals with regard to the processing of their personal data and the free flow of personal data within the European Union (EU).[9] Over the last two decades, the Directive has been the central data protection legislation in the EU.[10] However, the developments in information technology (e.g. Big Data and new analytical technologies) have raised new concerns with regard to the efficacy of the Directive.[11] In the light of these developments, the European Commission presented a package of proposals to update and modernize the EU data protection framework, this included a proposal for the General Data Protection Regulation (GDPR). After intense discussions between the European Commission, Parliament, and Council, the Regulation was adopted in December 2015 and will enter into force in all EU Member States in May 2018. The aim of the Regulation is to reinforce data protection rights of individuals, facilitate the free flow of data in the digital single market of the EU and reduce administrative burden.[12] The Regulation holds on to the main elements of the Directive, a fact that is being criticized by many legal scholars (e.g. Mantelero[13] and Pearce[14]).

Profiling is an issue that is dealt with more extensively in the new Regulation than in the old Directive. Although already included in Article 15 DPD, the Directive did not mention the term profiling as such. Article 15 DPD protected individuals against decisions based solely on automated processing of data intended to evaluate certain personal aspects, for example relating to their performance at work. Given the issues arising around the concept of profiling, in particular in relation to Big Data, the Regulation does provide a definition of profiling in Article 4(4) GDPR similar to the one already stated in the Directive. The fact that the Article 29 Working Party has recently published Guidelines on Automated individual decision-making and Profiling for the purpose of the Regulation showed that profiling is a hot issue.[15]

1.2 Significance

As mentioned before, profiling could have strong impacts on individuals' rights and freedoms and on society as a whole. Profiling can lead to discrimination, information asymmetries, and de-individualisation.[16] But also to issues concerning surveillance, privacy-intrusive commercial

[8] Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281.

[9] ibid., Article 1.

[10] Christina Tikkinen-Piri, Anna Rohunen and Jouni Markkula, 'EU General Data Protection Regulation: Changes and Implications for Personal Data Collecting Companies' (2018) 34 Computer Law & Security Review 134.

[11] Pearce (n 2).

[12] 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) [2012] COM(2012)/0011.

[13] Alessandro Mantelero, 'Regulating Big Data. The Guidelines of the Council of Europe in the Context of the European Data Protection Framework' (2017) 33 Computer Law and Security Review 584.

[14] Pearce (n 2).

[15] Article 29 Working Party, 'Guidelines on Automated individual decision-making and Profiling for the purpose of the Regulation 2016/679' 17/EN WP 251, 3 October 2017.

[16] Schermer (n 3).

solicitations, security risks and exposure to hidden unfair commercial practices.[17] Especially in this Big Data era the rights and freedoms of individuals are at stake. Big Data are datasets which are so large and complex they cannot be stored and processed using standard statistical software or analysed in a single organization. This concept makes it very difficult for a person to keep track of every data processing activity which includes his or her data. Additionally, this makes it very hard to assess whether the data controller acts in compliance with the applicable legal standards.[18]

One of the main problems with the EU regulatory framework and Big Data is the notion of "specified purpose". Big Data undermines this notion, which is of high importance in the GDPR, as with Big Data the purposes of data collection have become vague or extremely broad.[19] Furthermore, the Regulation shows a shift to individual self-determination in the form of Data Protection Impact Assessments. In principle, this reduces the difficulties of regulating Big Data. However, these DPIAs are related to the use of data for a specific purpose.[20] It is interesting to take into against the new Guidelines by the CoE on the processing of personal data in a Big Data world.

In summary, Big Data imposes great challenges to the current legal framework on privacy and data protection effective in Europe (both EU and CoE). It is important that governments and businesses do everything to effectively implement the provisions provided.

1.3 Central research question and sub-questions

The central research question of this thesis is: *"Do the current data protection frameworks of the Council of Europe and the European Union adequately regulate the data protection issues posed by profiling using Big Data, and if not, how could these issues be addressed adequately?"* In order to give an adequate, sufficient and comprehensive answer to the central research question the following sub-question will be discussed:

- What is Big Data? And what is profiling? How are these two linked?
- How do the EU and CoE data protection framework address profiling and Big Data?
- Which fundamental rights issues do profiling in relation to Big Data cause?
- Are the EU and CoE data protection frameworks able to deal with these issues? And how can individuals' rights be adequately protected in these systems?

1.4 Overview of the chapters

Following the order of the sub-questions, Chapter 2 will focus on the definitions of Big Data and profiling in Convention 108. In particular, the chapter includes an analysis of the provisions as formulated in Convention 108 and the GDPR as well as an analysis of the amendments made

[17] Nancy J King and Jay Forder, 'Data Analytics and Consumer Profiling: Finding Appropriate Privacy Principles for Discovered Data' (2016) 32 Computer Law & Security Review 696.

[18] Bart van der Sloot, 'How to Assess Privacy Violations in the Age of Big Data? Analysing the Three Different Tests Developed by the ECtHR and Adding for a Fourth One' (2015) 24 Information & Communications Technology Law 74.

[19] Tal Z Zarsky, 'Incompatible: The GDPR in the Age of Big Data' (2017) 47 Seton Hall L. Rev. 27.

[20] Mantelero (n 13).

to the definition of profiling in the last decade. Additionally, the concept of Big Data will be explained in detail and the usage of Big Data in relation to profiling will be elaborated. Finally, the link between Big Data and profiling is discussed. Chapter 3 sets out the privacy and data protection framework of the CoE. Chapter 4 deals with the consequences of profiling as such, and the abuse or misuse thereof, for individuals and society. The focus will be on fundamental rights issues, especially with regard to privacy and data protection. The challenges to the legal framework of the aforementioned issues will also be discussed, and next, a recommendation will be made on how individuals' rights could be adequately protected in these systems. Finally, Chapter 5 will consist of a conclusion about the research conducted throughout this thesis.

1.5 Methodology

The purpose of my research is to conduct an extensive legal analysis of the existing legal framework on profiling in the age of Big Data in order to find out whether it provides adequate protection to individuals. This analysis will include mainly European Law, namely the DPD, the GDPR, Convention 108 and the Consultative Committee of Convention 108 Guidelines on the Protection of Individuals with regard to the Processing of Personal Data in a World of Big Data. Additional information will be gathered through articles of (legal) scholars, relevant documents, and opinions of public and private bodies and relevant case law. The main research technique used is comparative.

Chapter 2 – Defining Big Data and Profiling

2.1 Introduction

Big Data is a well-known term, but what does it mean? Its definition is subject to debate. Big Data and profiling are both well-known terms, but what do they mean? Is its key characteristic the volume of the databases, its complexity, or the speed of the data gathering and processing? In that regard, profiling has a more generally accepted definition. In this chapter, the definitions of Big Data and profiling as they will be used throughout this thesis will be set out. Furthermore, the different applications of Big Data and profiling will be discussed in detail. With regard to the central research question of this thesis, it is important to define the relevant uses of Big Data, especially with regard to profiling. Additionally, the opportunities and challenges of Big Data will be discussed. The challenges in particular form an important ground for the research conducted in this thesis. Finally, the link between Big Data and profiling will be explained.

2.2 Big Data

2.2.2 Definition of Big Data

In order to create a better understanding of the term Big Data, it is helpful to put it in a practical perspective. For example, the company Netflix uses its customer data (with more than 100 million customers worldwide this is a huge amount of data) to predict viewing preferences and deliver personalized recommendations. It even uses the data to help determine which new TV series and movies it should create.[21] Another example is the running and cycling application Strava, which generated a global heatmap based on the data of their "athletes". The global heatmap is a direct visualisation of their athlete network.[22] Furthermore, Big Data is used to determine a user's friend recommendations on Facebook and to point out suggested purchases on websites like Bol.com.

Big Data has been defined in several different ways in academic literature. In this paragraph four of these definitions will be discussed. First, the definition that was given to Big Data by the Art. 29 Working Party (WP). The Art. 29 WP refers to the phenomenon of Big Data as the exponential growth in availability and automated use of information. Big Data itself is defined as the *"gigantic digital datasets held by corporations, governments and other large organisations, which are then extensively analysed using computer algorithms"*.[23] Second, the definition of the European Data Protection Supervisor (EDPS). The EDPS refers to Big Data as *"the practice of combining huge volumes of diversely sourced information and analysing them, using more sophisticated algorithms to inform decisions"*. The EDPS points out that not all Big Data collected and used is personal data, but the monitoring of human behaviour is one

[21] David Carr, 'Giving Viewers What They Want' *The New York Times* (24 February 2013) <www.nytimes.com/2013/02/25/business/media/for-house-of-cards-using-big-data-to-guarantee-its-popularity.html?pagewanted=all&_r=0>

[22] Strava: The Global Heatmap, Now 6x hotter. Available online: <https://medium.com/strava-engineering/the-global-heatmap-now-6x-hotter-23fc01d301de>

[23] Article 29 Working Party, 'Opinion 03/2013 on purpose limitation' 00569/13/EN WP 203, 2 April 2013.

of the most useful applications of Big Data for businesses and governments.[24] Third, perhaps the most well-known definition amongst the public, the definition of Big Data created by Gartner.[25] This definition is also known as the 3V model, the 3Vs being: volume, velocity and variety. They refer to the amount of data processed, the speed of the data processing, and the range of data types and sources.[26] And fourth and most relevant for this thesis, the definition followed by the Consultative Committee of Convention 108. The Consultative Committee takes a slightly different approach by encompassing both Big Data and Big Data Analytics in its definition. Big Data are *"a paradigm for enabling the collection, storage, management, analysis and visualization, potentially under real-time constraints, of extensive datasets with heterogeneous characteristics"*. The term Big Data Analytics *"refers to the whole data management lifecycle of collecting, organizing and analysing data to discover patterns, to infer situations or states, to predict and to understand behaviour"*.[27] When analysing all these definitions it can be concluded that Big Data has three defining features that need to be taken into account. The first feature is the availability of data at a massive scale. This data is collected not only online, but also through the use of location tracking on mobile devices and thousands of apps that share data with multiple parties. The second feature is the use of high speed. By coupling high-transfer rate computers with petabytes of storage capacity, data can be processed cheaply and efficiently. The third feature is the use of new computational frameworks. Through these frameworks the huge volume of data is stored and analysed.[28]

Finally, it is important to gather some insights on the usage of Big Data. Although it could be used in almost every sector, its usage can generally be divided into three types. Firstly, the use of Big Data by the government for specific tasks. For example, the use of Big Data by the intelligence services, the police or the tax authorities. Secondly, the use of Big Data by the private and semi-public sector. The main purpose of their usage is helping or facilitating them in achieving specific tasks and/or goals. For example, companies (like Netflix) use Big Data to personalize services and advertisements.[29] But Big Data is also widely used in healthcare. By assisting doctors and healthcare professionals in their decision-making processes, the efficiency and quality of healthcare operations can be improved.[30] Thirdly, the use of Big Data by both the government and private sector companies to improve their services to citizens and customers. For example, by increasing the transparency of their activities.[31]

---

[24] European Data Protection Supervisor, 'Opinion 7/2015 on meeting the challenges of big data', 19 November 2015.

[25] Gartner is the world's leading research and advisory company. For more info see: <www.gartner.com/technology/about.jsp>

[26] Gartner IT Glossary: Big Data. Available online: <www.gartner.com/it-glossary/big-data>

[27] Consultative Committee of Convention 108, 'Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data' T-PD(2017)01, 23 January 2017 (Big Data Guidelines).

[28] Ira S Rubinstein, 'Big Data: The End of Privacy or a New Beginning?' (2013) 3 International Data Privacy Law 74.

[29] Bart van der Sloot and Sascha van Schendel, 'Ten Question for Future Regulation of Big Data: A Comparative and Empirical Legal Study' (2016) 7 JIPITEC 110.

[30] Tilman Becker, 'Big Data Usage' in José María Cavanillas, Edward Curry and Wolfgang Wahlster (eds), *New Horizons for a Data-Driven Economy* (Springer International Publishing 2016) <http://link.springer.com/10.1007/978-3-319-21569-3_8> accessed 5 April 2018.6/8/2018 1:50:00 PM

[31] Van der Sloot and Van Schendel (n 8).

2.2.3 Big Data Value Chain

In itself data does not have that much value, it is through the Big Data value chain that it gathers its worth.[32] This value chain consists of the following phases; data acquisition, data analysis, data curation, data storage and data usage.[33] Below, the different phases of this value chain will be discussed. In the data acquisition phase, data is gathered, filtered and cleaned. After this, it will be put in a data warehouse (or any other storage solution) in which the data analysis can be carried out.[34] Distinctly for Big Data is that usually large amounts of data are gathered from all sorts of sources, without knowledge about what will be done with the data in the future.[35] Data analysis is the phase in which the raw data acquired is turned into useful information for decision-making processes, as well as domain-specific usage.[36]After this comes the phase of data storage, which is the continuous management of the data, preferably in a scalable way.[37] However, this is not always easy. The production of data is increasing faster than the storage capacity.[38] Finally, the phase of data usage. Herein, the data is integrated into the data-driven business activities such as automated decision-making and profiling.[39] Data curation occurs throughout the whole life-cycle of the data and is the active management of the data in order to ensure the necessary quality for its effective usage.[40] It is important to keep in mind that these phases do not necessarily occur in this order, the process often occurs in loops.[41] For example, a data analysis can result in the acquisition of more data.

2.2.4 Opportunities and challenges of Big Data

Big Data and Big Data analytics both have opportunities and challenges. The opportunities of Big Data have already been discussed briefly as they follow from the application of Big Data. With regard to services provided to citizens and customers, Big Data will support the improvement of services to citizens and customers, could improve (corporate) transparency and provide individuals with more control. Furthermore, the main reason why the corporate world

---

[32] Commissie voor de bescherming van de persoonlijk levenssfeer, *Big Data Rapport* (February 2017). Available online: <www.privacycommission.be/sites/privacycommission/files/documents/Big_Data_Rapport_2017.pdf>

[33] Edward Curry, 'The Big Data Value Chain: Definitions, Concepts, and Theoretical Approaches' in José María Cavanillas, Edward Curry and Wolfgang Wahlster (eds), *New Horizons for a Data-Driven Economy* (Springer International Publishing 2016) <http://link.springer.com/10.1007/978-3-319-21569-3_3> accessed 9 May 2018.

[34] ibid.

[35] Commissie voor de bescherming van de persoonlijk levenssfeer, *Big Data Rapport* (February 2017). Available online: <www.privacycommission.be/sites/privacycommission/files/documents/Big_Data_Rapport_2017.pdf>

[36] Curry (n 33).

[37] ibid.

[38] EMC Digital Universe with Research & Analysis by IDC, *The Digital Universe of Opportunities: Rich Data and the Increasing Value of the Internet of Things* (April 2014). Available online: <www.emc.com/collateral/analyst-reports/idc-digital-universe-2014.pdf>

[39] Curry (n 33).

[40] ibid.

[41] Commissie voor de bescherming van de persoonlijk levenssfeer, *Big Data Rapport* (February 2017). Available online: <www.privacycommission.be/sites/privacycommission/files/documents/Big_Data_Rapport_2017.pdf>

is interested in Big Data is the fact that it could lead to substantial growth in companies, jobs and profits generated (of course this is also interesting for governments and other public organisations). Additionally, it could help organizations, institutions and government departments in achieving specific objectives.[42] As an illustration a few practical examples will be set forth. Google Flu for example, predicts and locates flu outbreaks which could support the containment of the outbreak. Another example is the smart grid which enables electricity service providers, users and other third parties to monitor and control electricity use. Hence, help to lower customers' electricity use and give providers insights in the energy demand.[43]

Besides the opportunities of the use of Big Data, its usage also poses challenges mainly regarding privacy. The EDPS has several concerns with regard to Big Data. One of them is the lack of transparency. According to the EDPS, the processing of data is getting more complex, whilst organisations are claiming secrecy on grounds of commercial confidentiality. Moreover, the EPDS fears an informational imbalance between individuals and the users of Big Data. When these issues are not adequately addressed the EDPS fears that they will have a negative impact on the rights and freedoms of individuals.[44] The Consultative Committee of Convention 108 also addresses some of the risks related to the use of Big Data. It points out that there is an underestimation of the legal, social, and ethical implications of the use of Big Data for decision-making purposes. It could also lead to biases in data analysis. Furthermore, it could have negative effects on the informed involvement of the individuals concerned.[45] To conclude, the risks stipulated by the Article 29 WP will be set forth. The Article 29 WP does not go into too much detail about these risks, however they are more than interesting to mention. The Article 29 WP sees the increased possibilities of government surveillance by the use of Big Data as a risk to the protection of personal data and the right to privacy. The use of Big data could also lead to inaccuracy, discrimination, exclusion and economic imbalance according to the Article 29 WP. These concerns are raised in particular, when algorithms spot correlations and subsequently draw statistical inferences. When applied to inform marketing or other decisions, these inferences might turn out to be unfair and discriminatory. This may contribute to the existence of certain prejudices and stereotypes. The possible increase of economic imbalance is mainly between large corporations using extensive datasets and sophisticated analytical tools on the one hand, and the consumers on the other hand. As well as the EDPS, the Article 29 WP also points out the lack of transparency as a serious concern. Individuals become less and less empowered when it comes to data processing due to a lack of understanding and control. Finally, the mere scale of data collection, tracking and profiling is a reason for concern, as is the lack of data security.[46]

[42] van der Sloot and van Schendel (n 29).

[43] Omer Tene and Jules Polonetsky, 'Privacy in the Age of Big Data: A Time for Big Decisions' (2012) 64 Stanford Law Review Online 63.

[44] European Data Protection Supervisor, 'Opinion 7/2015 on meeting the challenges of big data', 19 November 2015.

[45] Consultative Committee of Convention 108, 'Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data' T-PD(2017)01, 23 January 2017 (Big Data Guidelines).

[46] Article 29 Working Party, 'Opinion 03/2013 on purpose limitation' 00569/13/EN WP 203, 2 April 2013.

2.3 Definition of profiling

The concept of profiling occurs in a diversity of contexts: from criminal investigation to marketing research, from supply chain management to supporting justice, from anti-terrorism to direct marketing. All these contexts share at least one common characteristic, namely the fact that they use algorithms or other techniques to derive knowledge from huge sets of data.[47] Already in the early 1980s, Gary T. Marx, as one of the first scholars, tried to define profiling. According to Marx, profiling is "*seeking clues that will increase the probability of discovering infractions relative to random searches."*[48] Over the course of the years, technical developments asked for a broader, and more specific definition of profiling. Among scholars, a general accepted definition is that of Mireille Hildebrandt:

> *"the process of 'discovering' correlations between data in databases that can be used to identify and represent a human or non-human 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".*[49]

Hildebrandt's definition is very diverse and encompasses many forms of profiling. Profiling can be either automated or non-automated, can be applied to a group or individual, and can be direct or indirect. A further distinction can be made between organic, human and machine profiling.[50]

Besides the definition given by scholars, the Consultative Committee and the Committee of Ministers of the CoE have also defined profiling. Unlike the GDPR, Convention 108 does not contain specific provisions on automated decision-making or profiling. With the emergence of the use of numerous technologies (such as bugs and cookies) providing the possibility to observe and trace individuals without their knowledge the need for a clear legal framework grew.[51] The arrival of the internet made it possible to link individuals and institutions. First through webservers, emails and blogs, but nowadays more and more via social media and the interlinking of smart devices (IoT). This significant growth in data storage, processing and communication has led to the gathering of huge amounts of information on broad population groups in large databases and finding the correlations between them. Thus,

---

[47] Mireille Hildebrandt, 'Defining Profiling: A New Type of Knowledge?' in Mireille Hildebrandt and Serge Gutwirth (eds), *Profiling the European Citizen* (Springer Netherlands 2008) <http://link.springer.com/10.1007/978-1-4020-6914-7_2> accessed 5 April 2018.

[48] Gary T Marx and Nancy Reichman, 'Routinizing the Discovery of Secrets: Computers as Informants' (1984) 27 American Behavioral Scientist 423.

[49] Mireille Hildebrandt, 'Defining Profiling: A New Type of Knowledge?' [2008] Profiling the European Citizen: Cross-Disciplinary Perspectives 17.

[50] ibid.

[51] Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, 'Application of Convention 108 to the profiling mechanism' T-PD(2008)01, 11 January 2008.

creating the possibility to construct a group of 'profiles' that can be applied to classify individuals within the given 'profiles' and to predict their future behavior.[52]

In 2008, the Consultative Committee published a report on the application of Convention 108 to the profiling mechanism.[53] The Consultative Committee makes a distinction between abstract and specific profiling. Abstract profiling is the process of identifying information, making predictions and inference. Specific profiling is "*based on the collection and analysis of information about specific individuals, with no inference or prediction based on external sources.*"[54] In any case, specific profiling falls within the scope of application of Convention 108 due to the fact that personal data is used. Thus, the individuals or groups of individuals concerned have the rights that are specified in Convention 108.[55] The Consultative Committee sets out three stages that need to be fulfilled in order to speak of profiling. First, the stage of data warehousing. In this stage, large quantities of personal and anonymous data are collected with the goal of creating an anonymous data set describing certain aspects of the personality of an unidentifiable individual. Second, the stage of data mining. Statistical methods are carried out with the purpose of determining the probability of correlations between certain observable variables. The outcome of this stage is a mechanism in which individuals are categorised on the basis of these variables in order to derive other information regarding individuals that are not observable. Unavoidably, there is a certain margin of error in this process. And third, the stage of inference. In this stage, the mechanism described above is used to infer past or new characteristics or past, present or future behavioural variables, based on variables and characteristics of an individual identified in general terms. In the conclusion of the report, the Consultative Committee recommends that the CoE to prepare a recommendation setting out the rules of profiling activities.[56] And so, in 2010, the Committee of Ministers of the CoE published the Recommendation on the protection of individuals with regard to automatic processing of personal data in the context of profiling.[57] The Recommendation follows the stages of profiling as set out by the Consultative Committee. Moreover, it provides clear definitions of the terms profile and profiling. Profile means "*a set of data characterizing a category of individuals that is intended to be applied to an individual.*" Profiling means "*an automatic data processing technique that consists of applying a "profile" to an individual, particularly in order to take decisions concerning her or him or for analyzing or predicting her or his personal preferences, behaviors and attitudes.*"[58] As this is the most recent definition of profiling given by the CoE, this will be the definition that will be used throughout this thesis.

---

[52] Committee of Ministers of the Council of Europe, *The protection of individuals with regard to automatic processing of personal data in the context of profiling* (October 2011, ISBN 978-92-871-7074-3), Strasbourg: Council of Europe Publishing (Rec(2010) 13). Available online: <https://rm.coe.int/16807096c3>

[53] Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, 'Application of Convention 108 to the profiling mechanism' T-PD(2008)01, 11 January 2008.

[54] ibid.

[55] ibid.

[56] ibid.

[57] Committee of Ministers of the Council of Europe, *The protection of individuals with regard to automatic processing of personal data in the context of profiling* (October 2011, ISBN 978-92-871-7074-3), Strasbourg: Council of Europe Publishing (Rec(2010) 13). Available online: <https://rm.coe.int/16807096c3>

[58] ibid.

Finally, it is important to understand the different uses and effects of profiling. First, profiling can be used as a selection instrument to decide which persons or groups deserve more attention. Second, it can be used as an instrument in decision-making. Third, profiling can be used as a tool to support detection of for example people that are breaking or will be breaking the rules. And fourth, it is an instrument for evaluating practices and intervention.[59] In my opinion, these four uses of profiling give a good overview of its usage in general. Finally, the people affected by profiling can be distinguished in three groups: the people whose data is used to create the profiles, the people to which the profile applies, and the people who are subject to the automated decision-making based on the profile.[60]

2.4 The link between Big Data and profiling

With the definitions of Big Data and profiling in mind, it is now interesting to look at the link between the two. The most widespread view about the link between Big Data and profiling is the fact that profiling using Big Data magnifies the impact of profiling and puts more pressure on the checks and balances in the legal framework.[61] For example, the European Commission states that the main advantage of Big Data is that it can enable useful insights by revealing patterns between different sources and data sets.[62] In their article, De Hert & Lammerant explain that Big Data creates new visibilities. In former times, train tickets were anonymous whereas now our personal public transportation cards track our every move. Furthermore, due to the changes in data aggregation and collection methods it becomes possible to link existing data sources and make them inter-operable.[63]

2.5 Conclusion

In this chapter, the concepts and uses of Big Data and profiling are defined. Big Data's well-known definition follows from the 3V model: volume, velocity, and variety. The Consultative Committee of Convention 108 has defined Big Data as the collection, storage, management, analysis and visualizations of extensive datasets. Big Data analytics consists of the analysis of these data sets to discover patterns, inform situations and to understand and predict behaviour. The three defining features of Big Data are the availability of data, the high speed of the data processing and the use of new computer frameworks. Big Data is used for various purposes by governments and the semi-public and private sector. It is used to fulfil specific tasks, achieve certain goals, and to improve services. Profiling is an automatic data processing technique that, through the use of profiles of an individual, makes decisions concerning this person. But it can also be used for analyzing this person's preferences, behaviour or attitude. The use of Big Data

[59] Bart Custers, 'Risicogericht toezicht, profiling en Big Data' (2014) 5 Tijdschrift voor Toezicht 9.

[60] Hans Lammerant and Paul De Hert, 'Predictive Profiling and Its Legal Limits: Effectiveness Gone Forever' in B van der Sloot, D Broerders and E Schrijvers (eds), *Exploring the boundaries of big data*, vol 32 (Amsterdam University Press 2016).

[61] ibid.

[62] European Commission, *The EU Data Protection Reform and Big Data Factsheet* (January 2016, ISBN 978-92-79-60478-2), Luxembourg: Publications Office. Available online: <http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=52404>

[63] Lammerant and De Hert (n 60).

in the context of profiling magnifies its impact. In the next chapter, the data protection framework of the Council of Europe will be set out.

Chapter 3 - The European data protection framework

3.1 Introduction

In this chapter, the legal framework of the EU and the CoE will be set forth. In order to be able to give an extensive answer to the central research question, it is essential to understand the place of Big Data and profiling in the legal framework. Therefore, the data protection framework of the EU, especially the GDPR and to a lesser extent the DPD, will be scrutinized. Furthermore, the data protection of the CoE will be set out. Including, an in-depth analysis will be made of the "Recommendation on the protection of individuals with regard to automatic processing of personal data in the context of profiling" and the "Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data".

3.2 European Union

3.2.1 General Data Protection Regulation

In 1995, the EU adopted its main instrument on data protection, Directive 95/46/EC, better known as the Data Protection Directive (DPD).[64] The aim of the DPD was the harmonization of national data protection laws.[65] The DPD draws on the possibility, provided for in Article 11 of Convention 108, to foresee a wider measure of protection than that of the Convention itself. It builds on the principles of the right to privacy contained in Convention 108. However, due to technical progress and globalization, the way in which our personal data is collected, accessed and used has changed. These developments asked for new data protection legislation. Therefore, in 2009, the European Commission (EC) started a public consultation about the amendment of the DPD. Finally, in 2012, the European Commission (EC) proposed a comprehensive reform of the DPD in order to strengthen online privacy rights and boost Europe's digital economy.[66] As of 25 May 2018, the new General Data Protection Regulation (GDPR) entered into force.[67] It is interesting to point out the choice of instrument, a Regulation, which means that the GDPR is directly applicable in all EU Member States. It seems that legislators no longer perceive data protection to be a local phenomenon but rather an EU concern that needs to be regulated directly at the EU level.[68] The key principles of data protection law have been maintained in the GDPR, but it also entails many changes and additions. Some of the main changes include an increased territorial scope, strengthened

[64] Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281.

[65] ibid. Recital 7 and 8.

[66] The History of the General Data Protection Regulation. Available online: <https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en>

[67] Regulation (EU) 2016/679 of the European Parliament and 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) [2016] OJ L 119.

[68] Paul de Hert and Vagelis Papakonstantinou, 'The New General Data Protection Regulation: Still a Sound System for the Protection of Individuals?' (2016) 32 Computer Law & Security Review 179.

conditions for consent, the right to be forgotten, the principle of accountability, privacy by design and privacy by default. The GDPR does not contain a provision on Big Data, nor does it provide a definition.

Under Article 68 of the GDPR, a European Data Protection Board has been established as the successor of the Article 29 Working Party (WP) of the DPD. It is an important actor in ensuring the application of data protection rules throughout the EU. The main tasks of the EDPB are to ensure consistency, to provide consultation and to give guidance to the Commission and the supervisory authorities.[69] Over the course of the years, the Article 29 Working Party (WP) has developed an extensive framework of e.g. Opinions, Guidelines and Recommendations that provide the community guidance in the application of the DPD (and GDPR).[70] Early 2018, the Article 29 WP published an updated set of "Guidelines on Automated individual decision-making and Profiling for the purposes of the GDPR" which are particularly relevant to this thesis. These guidelines will be discussed extensively in the next paragraph.

3.2.2 Profiling in the General Data Protection Regulation

Profiling is defined in Article 4(4) GDPR and consists of three elements. It needs to be a form of automated processing, carried out on personal data to evaluate personal aspects about a natural person.[71] The GDPR speaks of 'any form of automated processing', which means that human involvement does not necessarily cause the inapplicability of the Regulation. Evaluation of personal aspects suggests that profiling needs to involve some form of assessment or judgement about a person.[72] The definition of profiling in the GDPR is inspired by Recommendation CM/Rec (2010)13 but is not identical to it. Whereas the GDPR's definition includes processing that does not include inference, the Recommendation does not.[73] However, the Recommendation sets out three distinct stages which might involve profiling; "*data collection, automated analysis to identify correlations, and applying the correlation to an individual to identify characteristics of present or future behavior*".[74] Data controllers must ensure compliance with the GDPR requirements in all of these stages. Another concept that is important with regard to profiling is automated decision-making. Profiling may take place without making automated decision, as automated decisions can be made with or without profiling.[75] But they cannot be seen as completely separate activities, an automated decision-making process can become profiling. Whether data controllers are carrying out profiling,

---

[69] EU Agency for Fundamental Rights and Council of Europe, *Handbook on European data protection law (2018 edition)* (April 2018, ISBN 978=92-871-9849-5), Luxembourg: Publications Office of the European Union. Available online: <https://publications.europa.eu/en/publication-detail/-/publication/5b0cfa83-63f3-11e8-ab9c-01aa75ed71a1>

[70] Regulation (EU) 2016/679 of the European Parliament and 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) [2016] OJ L 119, Article 68 GDPR.

[71] ibid. Article 4(4).

[72] Article 29 Working Party, 'Guidelines on Automated individuals decision-making and Profiling for the purposes of Regulation 2016/679', 17/EN WP 251, 6 February 2018.

[73] ibid.

[74] ibid.

[75] ibid.

automated decision-making or both, they need to comply with the principles of the GDPR and have a lawful basis for the processing.

Profiling can be used in three different ways: general profiling, decision-making based on profiling, and solely automated decision-making including profiling under Article 22 GDPR.[76] All profiling and automated decision-making activities performed by data controllers need to comply with the key data protection principles of Article 5 GDPR. These consist of lawful, fair and transparent processing, the purpose limitation principle, data minimization, and storage limitation. Furthermore, one of the lawful bases for processing of Article 6 GDPR needs to be met. Profiling in the sense of Article 22 GDPR has to meet additional criteria. Article 22 GDPR encompasses the right of data subjects "*not to be subject to be based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her*". This is a general prohibition for decision-making based solely on automated processing, the data subject does not need to take action regarding the processing of their personal data. The wording 'based solely' on automated processing means that there is no human involvement in the decision-making process. Nonetheless, data controllers cannot get around this provision by a token gesture of human involvement.[77] There needs to be meaningful oversight of the decision by someone with the authority and competence to change the decision.[78] Although the GDPR does not define 'legal' or 'similarly significant', the Article 29 WP has provided some guidance on their meaning. In order to speak of a legal effect, the decision must affect someone's legal rights, such as the freedom to associate with others. These rights can also result from a contract.[79] Whether a decision has 'similarly significantly affect' on the data subject is more difficult to determine. According to the Article 29 WP, the effects of the processing of personal data must be "*sufficiently great or important to be worthy of attention*".[80] This is potentially the case when the decision significantly affects the circumstances, behavior or choices of individuals, it prolongs or permanently impacts the data subject, or when it leads to the exclusion or discrimination of individuals. However, it remains difficult to determine precisely what can be considered to be 'similarly significant'.[81] The GDPR does provide three exceptions to the prohibition of Article 22. First, data controllers may use solely automated decision-making processes for contractual purposes if they believe it is the most appropriate way to achieve the objective of that contract.[82] Though, the data controller needs to prove that the use of a less privacy-intrusive method would not be sufficient.[83] Second,

[76] ibid.
[77] ibid.
[78] ibid.
[79] ibid.
[80] ibid.
[81] ibid.
[82] Regulation (EU) 2016/679 of the European Parliament and 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) [2016] OJ L 119, Article 22(2)(1).
[83] Article 29 Working Party, 'Guidelines on Automated individuals decision-making and Profiling for the purposes of Regulation 2016/679', 17/EN WP 251, 6 February 2018.

its use could be authorized by EU or Member State Law.[84] And third, if the data subject has given explicit consent for the automated decision-making including profiling.[85]

3.2.3 European Data Protection Supervisor

Besides the Article 29 WP and the EDPB, the EU also has an independent data protection authority in the form of the European Data Protection Supervisor (EDPS). The main responsibility of the EDPS is the monitoring of the application of the data protection rules by EU institutions and bodies.[86] As part of its duties, the EDPS advises all EU institutions and bodies on matters concerning the processing of personal data. In light of this, the EDPS has been developing the concept of 'Big Data protection'. In 2016, the EDPS published an "Opinion on coherent enforcement of fundamental rights in the age of big data". According to the EDPS, the use of Big Data technologies and services are an important stimulator of economic growth.[87] However, the users (e.g. companies and public institutions) of these services are not always aware of the impact of their operations on consumers. This results in a growing imbalance between consumers and service providers, which leads to diminished choice and innovation and a threat to the privacy of individuals.[88] The EDPS even goes as far by stating that the "*normative behaviour and standards now prevailing in cyberspace"* pose a threat to the rights of individuals as established in the EU Charter of Fundamental Rights.[89] The EDPS has incorporated three recommendations in their opinion. First, there is a need to better reflect the interests of individuals in Big Data mergers.[90] Second, there is a need to create a digital clearing house. With the creation thereof, the EDPS wants to create a platform for regulators active in the digital sector to come together and discuss important topics.[91] And third, there is a need to create an EU values-based common area on the web. In this area, individuals can interact without fear of being tracked.[92]

3.3 Council of Europe

3.3.1 Convention 108

Convention 108 is the only legally binding international instrument in the field of data protection. Whereas the EU Directives and Regulations are directly applicable in all EU countries, this is not the case for Convention 108, or CoE legislation in general. This means

[84] ibid. Article 22(2)(2).
[85] ibid. Article 22(2)(3).
[86] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data [2001] OJ L 8.
[87] European Data Protection Supervisor, 'Opinion on coherent enforcement of fundamental rights in the age of big data', Opinion 8/2016, 23 September 2016.
[88] ibid.
[89] ibid.
[90] ibid.
[91] ibid.
[92] ibid.

that CoE regulations are addressed to states in line with the standards of international conventions, implying a different and weaker binding nature. The purpose of Convention 108 was to secure the rights and fundamental freedoms for every individual in the territory of each Party.[93] In particular the right to privacy with regard to automatic processing of personal data relating to the individuals.[94] The Convention laid down basic principles for data protection, also referred to as the "common core" principles.[95] All of the Parties should take the necessary steps to give effect to these principles. The main goal of the Convention was to guarantee a minimum level of protection with regard to automatic processing of personal data in the Contracting States. Additionally, the implementation of the Convention needed to result in harmonization of the national laws of these States.[96] The difference between the EU and the CoE data protection framework lays within the taken approach. Where Convention 108 has a principle-based approach[97], the approach of the EU data protection framework relies more on detailed provisions.

In 2010, the CoE felt the need to update Convention 108 and started a modernization process. Throughout the modernisation process of both the EU and the CoE, regulators took the utmost care to ensure consistency and compatibility between the GDPR and the Modernised Convention 108.[98] The two key aims of the modernization are to address the challenges for privacy resulting from the use of new information and communication technologies and to strengthen the Convention's follow-up mechanism.[99] In September 2016, the CoE published a Draft Modernised Convention 108 that tries to achieve these aims.[100] On 18 May 2018, the Committee of Ministers adopted a Protocol amending Convention 108. The Protocol is opening up for signature on 25 June 2018.[101] With the adoption of this Protocol, the last step in the modernization process of the CoE has been fulfilled. The Modernised Convention 108 has reaffirmed important principles, whilst subsequently broadening the scope of data processing, providing new rights to individuals and increasing the responsibilities of data controllers and data processors.[102] Furthermore, the name and role of the Consultative Committee have been

[93] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (adopted 28 January 1981, entered into force 1 October 1985) ETS 108 (Convention 108), Article 1.
[94] ibid.
[95] Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS 108 (Explanatory Report to Convention 108).
[96] ibid.
[97] Jörg Plakiewicz, 'Convention 108 as a global privacy standard?' *International Data Protection Conference* (17 June 2011) <https://rm.coe.int/16806b294e>
[98] EU Agency for Fundamental Rights and Council of Europe, *Handbook on European data protection law (2018 edition)* (April 2018, ISBN 978-92-871-9849-5), Luxembourg: Publications Office of the European Union. Available online: <https://publications.europa.eu/en/publication-detail/-/publication/5b0cfa83-63f3-11e8-ab9c-01aa75ed71a1>
[99] Modernisation of the Data Protection "Convention 108". Available online: <www.coe.int/en/web/portal/28-january-data-protection-day-factsheet?desktop=true>
[100] Consolidated text of the modernisation proposals of Convention 108 finalised by the CAHDATA (meeting of 15-16 June 2016 (Draft Modernised Convention 108).
[101] Ad hoc Committee on Data Protection (CAHDATA), Protocol (CETS No. 223) amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) CM(2018)2-final, 18 May 2018.
[102] Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data (adopted 18 May 2018) CM/Inf(2018)15-final, Article 2(b) & (c), Article 5 and Article 9.

adjusted. Its name was changed to Convention Committee and it gained more power and functions.[103] Finally, the Convention underlines the need for independent supervisory authorities to play an important role in the effective enforcement of the Convention by Contracting Parties, this is key to its practical implementation.[104]

3.3.2 Recommendation on the protection of individuals with regard to automatic processing of personal data in the context of profiling

The Recommendation provides a list of principles that need to be taken into account by the governments of the Member States.[105] First, it is important that the data controller or processor that is carrying out the profiling upholds the individuals' fundamental rights and freedoms. In particular, their right to respect of privacy and prohibition of discrimination.[106] Second, Member States must promote the use of 'privacy by design' (taking privacy into account throughout the whole engineering process). Moreover, appropriate measures must be taken against the development and use of any technology designed to circumvent technical data protection measures aimed at protecting the respect of private life.[107] Additionally, the Recommendation sets out the conditions for the collection and processing of personal data in the context of profiling. Firstly, the collection and processing of personal data needs to be lawful. In that regard, Article 5 of Convention 108 needs to be followed closely[108], for example, the principle of purpose limitation.[109] The collection and processing of personal data that is used in the context of profiling should be adequate, relevant and not excessive in relation to the purposes.[110] This is especially important with regard to Big Data, as mentioned before the purpose is something that is difficult to define when collecting and processing personal data by Big Data usage. Subsequently, the quality of the data needs to be guaranteed. The data controller should correct data inaccuracy factors and limit the risks of errors inherent in profiling. Finally, it is prohibited to collect and process sensitive data in the context of profiling. However, there is an exception possible if these data are necessary for the lawful and specific purposes of processing, and as long as domestic law provides appropriate safeguards.[111]

3.3.3 Big Data Guidelines

Early 2017, the Consultative Committee of Convention 108 (replaced by the Convention Committee in the Modernised Convention 108) published a set of "Guidelines on the protection

[103] ibid., Article 4(3) and Article 22-24.

[104] EU Agency for Fundamental Rights and Council of Europe, *Handbook on European data protection law (2018 edition)* (April 2018, ISBN 978-92-871-9849-5), Luxembourg: Publications Office of the European Union. Available online: <https://publications.europa.eu/en/publication-detail/-/publication/5b0cfa83-63f3-11e8-ab9c-01aa75ed71a1>

[105] Committee of Ministers of the Council of Europe, 'Recommendation on the protection of individuals with regard to automatic processing of personal data in the context of profiling' Rec(2010)13, 23 November 2010.

[106] ibid.

[107] ibid.

[108] ibid.

[109] ibid.

[110] ibid.

[111] ibid.

of individuals with regard to the processing of personal data in a world of Big Data". Although the Guidelines only provide general guidance, they are the only ones of their kind on a European level and therefore provide an important step in regulating Big Data use.[112] According to the Committee, a large spectrum of Big Data concerns personal data with a direct impact on individuals and their rights with regard to the processing of personal data. Because of this, the Committee decided to draft these Guidelines.[113] The Guidelines address the fact that the emergence of the use of Big Data may be challenging for the application of some of the traditional data processing principles. These principles are the principle of data minimization, purpose limitation, fairness and transparency, and free specific and informed consent.[114] By suggesting a specific application of these principles in a Big Data context the Convention seeks to make them more effective in practice. The purpose of the Guidelines is to limit the risks of violating data subjects' rights by facilitating an effective application of the principles of the Convention in the Big Data context.[115] Where the DPD and GDPR are mainly addressed to the data controller, the Guidelines also concern the data processor to be an important asset for effective data protection.[116] According to the Guidelines, not only controllers but also processors should take into account the possible impact of the intended Big Data processing. Furthermore, they need to reckon with the broader ethical and social implications of this processing and safeguard human rights and fundamental freedoms.[117] Moreover, the processing of personal data should not clash with *"the ethical values commonly accepted in the relevant community or communities and should not prejudice societal interests, values and norms"*.[118] Although the Consultative Committee is aware of the fact that it might be difficult to define the ethical values, it provides some guidance by stating that the common ethical values can be found in international charters of human rights and fundamental freedoms.[119]

Principles and Guidelines

The basis of the data protection framework, provided for in the Big Data Guidelines, is formed by preventive policies and risk-assessment. In order to ensure the protection of individuals with regard to the processing of personal data, data controllers should adopt preventive policies. These policies should concern the risks of the use of Big Data and its impact on individuals and society.[120] The use of Big Data may affect the collective dimension of the right to privacy and the right to data protection. Hence, the preventive policies and risk-assessment should take into

[112] Mantelero (n 13). *There are several national Data Protection Authorities that provide guidance in the field of Big Data and data protection.
[113] Consultative Committee of Convention 108, 'Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data' T-PD(2017)01, 23 January 2017 (Big Data Guidelines).
[114] ibid.
[115] ibid.
[116] ibid.
[117] ibid.
[118] ibid.
[119] Mantelero (n 13).
[120] Consultative Committee of Convention 108, 'Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data' T-PD(2017)01, 23 January 2017 (Big Data Guidelines), para. 2.2.

account the legal, social and ethical impact of the use of Big Data. It is important that the controllers also include the right to equal treatment and to non-discrimination.[121] The Consultative Committee of Convention 108 considers a risk-assessment to be necessary in order to balance the protection of the fundamental rights and freedoms of individuals with the different interests that are affected by Big Data usage.[122] A risk-assessment generally contains three steps that need to be taken. First, the risks need to be identified and the potential impact of these risks need to be analysed.[123] Second, the measures to prevent or mitigate the risks need to be selected and adopted. These measures could be "by-design" or "by-default" solutions, which refer to *"appropriate technical and organisational measures taken into account throughout the entire process of data management"*. [124] And third, the effectiveness of the measures needs to be regularly reviewed.[125] The Guidelines also make an appeal to the individuals or groups that are potentially affected by the use of Big Data to get involved in the risk-assessment process.[126]

Most data protection frameworks, including the GDPR and Convention 108, are mainly focussed on the purpose limitation principle. Not only is it an essential first step for the application of data protection laws and for the design of adequate safeguards for any processing operation, but it is also a necessary principle for the application of other data quality requirements.[127] Article 5(b) of Convention 108 states that personal data can only be stored for specified and legitimate purposes. This means that it is not allowed to store data for undefined purposes. The legitimacy of the purpose may vary in accordance with national legislations.[128] The fact that State Parties can give their own interpretation to the meaning of legitimacy could lead to discrepancy between these State Parties on the content of the principle. Article 5(4)(b) of the Modernised Convention 108 states that personal data can be collected for specified, explicit and legitimate purposes. A specified purpose indicates that it is not permitted to process data for undefined, imprecise or vague purposes.[129] The legitimacy of the purpose still depends on the circumstances, but the Explanatory Report provides some more guidance than its predecessor. The objective is that in each instance the rights, freedoms and interests at stake need to be balanced, there is no reference to national laws.[130] With regard to the purpose limitation principle, the Big Data Guidelines follow Convention 108 by stating that personal data can only be processed for specified and legitimate purposes and may not be processed in ways incompatible with those purposes. Furthermore, they state that the further processing of personal data cannot be unexpected, inappropriate or otherwise objectionable to the data subject. Since Convention 108 did not mention the further processing of personal data, the

[121] ibid. para. 2.3.
[122] ibid. para. 2.4.
[123] ibid. para. 2.5(1).
[124] ibid. para. 2.5(2).
[125] ibid. para. 2.5(3).
[126] ibid. para. 2.5, 2.6 & 2.9.
[127] Article 29 Working Party, 'Opinion 03/2013 on purpose limitation' 00569/13/EN WP 203, 2 April 2013.
[128] Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS 108 (Explanatory Report to Convention 108).
[129] Explanatory Report to the Modernised Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data [CETS No. 223].
[130] ibid.

former Consultative Committee followed the Modernised Convention 108 on this point. Given the risk-based approach of the Guidelines, unexpected further processing contains the exposure of data subjects to greater or different risks than those anticipated by the initial purposes.[131] When putting the purpose limitation principle in a Big Data perspective, one could conclude that the processing of personal data using Big Data makes it difficult to determine the specific and legitimate purposes. However, this is not necessarily the case. Through Big Data applications large amounts of information from different sources are being collected and analysed to identify new trends and correlations in datasets. As a consequence, the purposes pursued by the analysis could be different from the initial purposes.[132] The Consultative Committee has taken this into account when drafting the Guidelines by acknowledging the *"transformative nature of the use of Big Data"*.[133] Hence, controllers should identify and inform data subjects about the potential impacts of the difference uses of their data on them.[134] Furthermore, the principle of transparency of data processing requires data controllers to publish the results of the risk-assessment process.[135] This provision is in line with Article 8(1)(b) of the Modernised Convention 108 which states that data controllers need to inform the data subjects about the purposes of the intended processing. Moreover, they need to inform them with any necessary additional information to ensure fair and transparent processing of the personal data.[136]

As previously stated, the measures to prevent or mitigate the risks raised by Big Data use could be "by-design" solutions. The Consultative Committee has pointed out the key elements that need to be taken in account by Big Data developers when adopting by-design solutions. First, the data controllers, and where applicable, processors should "*minimise the presence of redundant or marginal data"*.[137] Second, they should *"avoid potential hidden data biases"*.[138] Third, they should *"avoid the risk of discrimination or negative impact on the rights and fundamental freedoms of data subjects"*.[139] Data controllers (and processors) are advised to test the adequacy of the by-design solutions on a limited amount of data before applying them on large scale. Data controllers and processors are recommended to apply pseudonymisation measures, thus they can reduce the risks to data subjects.[140]

---

[131] Consultative Committee of Convention 108, 'Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data' T-PD(2017)01, 23 January 2017 (Big Data Guidelines), para. 3.1.

[132] Mantelero (n 13).

[133] Consultative Committee of Convention 108, 'Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data' T-PD(2017)01, 23 January 2017 (Big Data Guidelines), para. 3.2.

[134] ibid.

[135] ibid. para. 3.

[136] Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data (adopted 18 May 2018) CM/Inf(2018)15-final, Article 8.

[137] Consultative Committee of Convention 108, 'Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data' T-PD(2017)01, 23 January 2017 (Big Data Guidelines), para. 4.2.

[138] ibid.

[139] ibid.

[140] ibid. para. 4.3.

Convention 108 does not consider consent of the data subject as a legitimate ground for processing. However, the Modernised Convention 108 does take into account the notion of consent, as do the Guidelines. According to Article 5(2) of the modernization, data processing on the basis of free, specific, informed and unambiguous consent of the data subject should be possible. There are several aspects to this form of consent. The consent needs to be a free expression of an intentional choice given by a statement (written or oral) or a clear affirmative action.[141] Consent cannot be considered to be given by a data subject through silence, inactivity or pre-validated forms or boxes. It needs to concern all processing activities and show a clear indication of the acceptance of the proposed processing of personal data. Additionally, the data subject must be informed of the implications of the data processing.[142] In a Big Data context, it might be difficult to obtain the data subject's consent. Not all the processing activities might be known, and data controllers might even be unable to tell individuals what is likely to happen to their data.[143] The Guidelines provide a "*learn-from-experience*" approach to the notion of consent.[144] Acknowledging that the use of Big Data is very complex, the Consultative Committee gives data controllers the possibility of informing the data subject by using the results of the risk-assessment. The information might even be derived from a simulation of the effects of the use of the data and the potential impacts on the data subject.[145] Moreover, data subjects need to be able to react to processing that incompatible with the initial purposes and to withdraw their consent in an easy and user-friendly way.[146] When consent is required, imbalances in power between the data controller and the data subject can easily arise. Therefore, the data controller needs to prove that this imbalance does not exist.[147]

In a Big Data context, anonymization of personal data may not always have the desired results. Big Data has enabled the identification of data subjects using non-personal data, which puts pressure on anonymization as an effective data protection strategy.[148] The problem of re-identification is taken into account by the Consultative Committee. According to the Guidelines, the principles of data protection apply not only to the cases in which data enables the identification of data subjects, but also in cases of re-identification.[149] Data controllers should conduct an assessment of the risks of re-identification taking into account the time, effort, resources, context of use, costs and the available re-identification technologies. Besides

[141] Explanatory Report to the Modernised Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data [CETS No. 223].

[142] ibid.

[143] Article 29 Working Party, 'Opinion 03/2013 on purpose limitation' 00569/13/EN WP 203, 2 April 2013.

[144] Consultative Committee of Convention 108, 'Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data' T-PD(2017)01, 23 January 2017 (Big Data Guidelines), para. 5.1.

[145] ibid. para. 5.1.

[146] ibid. para. 5.2.

[147] ibid. para 5.3.

[148] IS Rubinstein, 'Big Data: The End of Privacy or a New Beginning?' (2013) 3 International Data Privacy Law 74.

[149] Consultative Committee of Convention 108, 'Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data' T-PD(2017)01, 23 January 2017 (Big Data Guidelines), para. 6.

this risk-assessment, the data controllers should also demonstrate that the measures they have adopted with regard to anonymization are adequate.[150]

The Guidelines also focus on the role of human intervention in Big Data-supported decisions. Given the complex nature of the use of Big Data and the possible effects decisions based on Big Data could have on individuals, data subjects might ask for reasoning underlying the processing. When decisions are made based on Big Data analytics all the circumstances should be taken into account, not merely the de-contextualized information of the data processing results. Moreover, the autonomy of human intervention in the decision-making process should be preserved when using Big Data.[151]

Finally, the concept of open data is addressed. Open data are *"any publicly available information that can be freely used, modified, shared and reused by anyone for any purpose, according to the conditions of open licenses."*[152] Big Data analytics makes it possible to extract inferences about individuals and groups through the use of open data. Therefore, public and private entities should reflect on their open data policies.[153] When data controllers are using different open data sets, it is important that they carefully take into account the principles of anonymization and the effects of merging and mining these different data.[154]

3.4 Conclusion

Convention 108 forms the basic data protection framework of the CoE. The Big Data Guidelines form a non-binding addition to this framework and are the only internationally recognized set of Guidelines on the protection of individuals with regard to processing in a Big Data world. The Guidelines consist of a set of principles and guidelines on the ethical and socially aware use of data; preventive policies and risk-assessment; purpose limitation and transparency; by-design approach; consent; anonymization; the role of the human intervention in Big Data-supported decisions; open data and education. The Recommendation is a similar non-binding instrument as the Big Data Guidelines. It provides guiding principles on how to conduct lawful profiling under Convention 108. The GDPR is the new data protection of Regulation of the EU. It sets forth a detailed framework of provisions that need to be taken into consideration when processing personal data in the EU. The Article 29 WP has provided a set of Guidelines that need to be considered by data controllers when conducting profiling. In the next chapter, the fundamental rights issues that might be caused by profiling using Big Data will be discussed.

[150] Ibid. para. 6.
[151] ibid. para. 7.
[152] ibid. Sector III.
[153] ibid. para. 8.1.
[154] ibid. para. 8.2.

Chapter 4 – Fundamental rights issues

4.1 Introduction

Profiling and data mining have proven to be very useful tools in dealing with the information overload in today's society. However, they also cause controversy.[155] In March 2018, Facebook and voter-profiling company Cambridge Analytica got widespread media attention for their involvement in Trump's presidential campaign. Cambridge Analytica harvested information from the Facebook profiles of over 50 million users without the consent of the Facebook users.[156] This information was used to build psychographic profiles which were used to make day-to-day campaign decisions, to help drive decisions on advertising and to decide on how to reach out to financial donors.[157] Of course, this case involves a serious data breach, but (Big Data) companies are gathering our personal data the whole time, at least this is what Facebook claims. The collected data is then used for purposes of profiling and Big Data analytics which are associated with a number of ethical and legal issues. In this chapter, these ethical and legal issues will be set out in addition to the ability of the EU and CoE data protection frameworks to deal with these issues. To conclude, some recommendations will be made on how individuals' rights could be adequately protected in these systems.

4.2 Fundamental rights issues

4.2.1 Fundamental values

Profiling and Big Data analytics provide information which enables parties to identify, target and act upon developments that are regarded unwanted, preferably before they occur. This could have several societal benefits such as tax fraud prevention and preventive policing. However, the downside of these benefits is that profiling poses significant risks to the fundamental values of our society.[158] According to Serge Gutwirth and Mireille Hildebrandt, profiling has a dark side. With this they mean that it makes "*invisible all what cannot be translated into machine-readable data"*.[159] As a result of this, the data collection phase of the decision-making process can be biased. Given the complexity of the applied algorithms, it is

[155] Bart W Schermer, 'The Limits of Privacy in Automated Profiling and Data Mining' (2011) 27 Computer Law & Security Review 45.

[156] Matthew Rosenberg, Nicholas Confessore and Carole Cadwalladr, 'How Trump Consultants Exploited the Facebook Data of Millions' *The New York Times* (17 March 2018) <www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html>.

[157] Stephanie Kirchgaessner, 'Cambridge Analytica Used Data from Facebook and Politico to Help Trump' *The Guardian* (26 October 2017) <www.theguardian.com/technology/2017/oct/26/cambridge-analytica-used-data-from-facebook-and-politico-to-help-trump>.

[158] Francesca Bosco and others, 'Profiling Technologies and Fundamental Rights and Values: Regulatory Challenges and Perspectives from European Data Protection Authorities' in Serge Gutwirth, Ronald Leenes and Paul de Hert (eds), *Reforming European Data Protection Law*, vol 20 (Springer Netherlands 2015) <http://link.springer.com/10.1007/978-94-017-9385-8_1> accessed 5 April 2018.

[159] Serge Gutwirth and Mireille Hildebrandt, 'Some Caveats on Profiling' in Serge Gutwirth, Yves Poullet and Paul De Hert (eds), *Data Protection in a Profiled World* (Springer Netherlands 2010) <www.springerlink.com/index/10.1007/978-90-481-8865-9_2> accessed 5 April 2018.

very difficult for human beings to intervene properly to mend the bias.[160] Organizations should pay attention to this as neglecting the bias could lead to ineffective and wrong decisions. In the worst-case scenario, the ignorance could lead to serious risks and damages to the population.[161] The cause of this is the non-transparent nature of the profiling and data processing activities. The limited transparency of profiling activities is a recurring problem. Citizens do not have proper access to the procedure behind the construction and application of profiles, whilst the parties employing data mining could gather valuable insights.[162] This can lead to information asymmetries between the government on the one hand, and the citizens on the other hand. With regard to the relationship between the government and citizens, it could give the government more actionable knowledge which could lead to more government power. With regard to the relationship between businesses and consumers, data mining can disturb the level economic playing field.[163]

In certain instances, Big Data analytics can be used to aid decision-making, but these decisions can be unwanted, unethical and illegal. Due to the limited transparency of Big Data analytics, it is unclear to people why and on what ground they are affected by a particular decision.[164] The governmental use of profiling seriously challenges the fundamental values of autonomy and self-determination. This is somewhat related to the risk of de-individualisation. In this light, self-determination must be seen as the control individuals need to have over the data and information produced by and on him or her.[165] As the example in the introduction to this chapter shows, the gathering of data in a digitized world happens in a non-transparent way undermining the self-determination and autonomy of individuals.

Classification and division are key elements of Big Data analytics.[166] Here, the risk is formed by the element of classification. As a result of the Big Data analytics, persons could be judged based on the characteristics of the group they form part of rather than on their own individual characteristics and merits.[167] These group profiles usually contain statistics and therefore are not per se valid for individuals as such. This can lead to stigmatisation and could damage societal cohesion.[168] An example of an application of profiling potentially doing harm is its use in healthcare. The gathering of information about patients' lifestyle creates the possibility to construct risk profiles which could be used by insurance companies to offer 'individual' insurance fees.[169] Hence, this undermines individuals' autonomy. Insurance companies will reward behaviours that are seen as low risk and 'healthy', whilst 'bad' behaviour that increases the risk of diseases could be sanctioned.[170]

---

[160] ibid.
[161] Schermer (n 155).
[162] ibid.
[163] ibid.
[164] ibid.
[165] Bosco and others (n 158).
[166] Schermer (n 155).
[167] Bosco and others (n 158).
[168] ibid.
[169] ibid.
[170] ibid.

Moreover, surveillance is one of the concerns. Big Data enables the gathering of large amounts of personal information of consumers who are not always aware of this. Privacy issues arise when the analysis of these datasets uncover non-obvious private information of the consumers that can also be used for profiling.[171] Next are the concerns related to data security.[172] The discovery of personal data and information through Big Data analytics which is subsequently used for profiling could expose consumers to a higher risk of online fraud or identity theft. Sources of personal identifiable data might seem appealing to thieves and the use thereof by such those thieves might expose consumers to higher threats of internet crime.[173]

Additionally, there is the concern of privacy-intrusive commercial solicitations. Through the usage of Big Data, tailored commercial solicitations can be sent to consumers. This could lead to the disclosure of painful or otherwise private information which for example happened in the United States.[174] Target, a big American retail chain, promoted pregnancy and baby-related products to a teenager. Based on her shopping behaviour they profiled her as being pregnant and due to the advertisements, her father found out about her pregnancy.[175] Furthermore, the concern of exposure to hidden unfair commercial practices arises.[176] As a result of Big Data analytics, businesses could find out which consumers are willing to pay higher prices for certain products than others. This has a number of consequences. Consumers can be worse off (paying more for a product then necessary) as the seller gains an unfair advantage (getting more returns for a product then usual). Moreover, the collected data could be inaccurate which could lead to erroneous statistical correlations and predictions. To conclude, there are no economic justifications for allowing commercial practices that involve price discrimination.[177]

Lastly, in its Opinion on 'Meeting the challenges of big data', the EPDS not only puts forth the legal threats of Big Data usage, but also explains the societal concerns that rise due to the use of Big Data. Big Data analytics enable the continuous tracking of online activity, this 'surveillance' may have "*a chilling effect on creativity and innovation*".[178] Furthermore, it is used for the statistic nature of identifying behaviour that poses less risk and generates more value for the entities processing the data. This practice tends to "*discourage or penalise spontaneity, experimentation or deviation from the statistical 'norm' and reward conformist behaviour."*[179] The EPDS is concerned that the constant tracking and analysing of our behaviour

---

[171] King and Forder (n 17).

[172] ibid.

[173] ibid.

[174] ibid.

[175] Kashmir Hill, 'How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did' (*Forbes*, 16 February 2012) <www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/#1db8bade6668>.

[176] King and Forder (n 17).

[177] Executive Office of the President of the United States, *Big Data and Differential Pricing* (February 2015), Washington D.C. Available online: <https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/docs/Big_Data_Report_Nonembargo_v2.pdf>

[178] European Data Protection Supervisor, 'Opinion 7/2015 on meeting the challenges of big data', 19 November 2015.

[179] ibid.

might influence it and might encourage us to act in a way that is deemed normative.[180] As a result of this, not only the right to privacy and data protection, but also the freedom of expression and the rights of free assembly and association could be supressed.

4.2.2 Fundamental rights

Profiling and data mining do not only pose risks to our fundamental values but also to our fundamental rights, especially to the right to privacy and data protection and the right to non-discrimination. First, the right to privacy and data protection. It is important to understand the scope of both these terms. Bosco et al. give a good explanation on how to understand these principles in the field of profiling. They state that "*while privacy is broader in the sense that privacy covers more than mere personal data the misuse of personal data can affect much more than someone's privacy.*"[181] There are certain privacy concerns that can be discussed in the light of discovered data, Big Data analytics and consumer profiling. Data protection is mentioned as one of the primary concerns. The likelihood of consumers being aware of, or their ability to exercise control over the production and use of the discovered data is relatively low.[182] This is related to the limited transparency of data mining. Because of this, it is difficult to prevent the misuse of the data that may cause significant harm. These privacy issues are not limited to data protection concerns but are also related to personal autonomy and liberty. This also hints back to the risk of information asymmetries as the consumer may not be aware of the profiling and does not have access to his or her profile.[183]

The second risk to our fundamental rights concerns the right to non-discrimination. This right is derived from the general principle of equality of Article 21 of the EU Charter of Fundamental Rights. In addition to this, specific provisions have been developed based on anti-discrimination legislation related to certain protected grounds. The distinction between direct and indirect discrimination is especially relevant in the field of profiling, since the violation of the right to non-discrimination due to the use of profiling rarely occurs directly on forbidden grounds. Usually, the classification and categorization that lead to an infringement of the right of non-discrimination are of a non-direct nature. When the focus of a data mining activity is ethnicity, religion or sexual preference, it always leads directly to discrimination. But even when the data mining is not focused on specific characteristics and thus is of a non-direct nature, it could lead to discrimination of certain groups. This is an issue as discrimination can be both unethical and illegal.[184] Due to the increasing capacities of Big Data usage and analytics the pressure on the concepts of privacy and data protection is increasing. Therefore, it is essential that an exhaustive privacy and data protection framework is established.

[180] ibid.
[181] Bosco and others (n 158).
[182] King and Forder (n 17).
[183] ibid.
[184] Schermer (n 155).

4.3 Pressure on the EU and CoE data protection frameworks

Considering the scholarly articles written on the issues of Big Data, there is a common theme that connects them. Almost all of the scholars regard the violation of the right to privacy and the right to data protection and the danger of discrimination as the main issues. How are these issues addressed by the EU data protection framework? The GDPR has established principles essential to both the data subjects and the data controllers. For the data controllers these include, among others, consent, purpose limitation and data minimisation.[185] The data subjects have certain rights that enable them to have access to their personal data, to rectify inaccurate personal data concerning them, and to demand erasure of data their personal data.[186] The previously stated fundamental rights issues challenge the legal instruments established to protect them, such as the GDPR and Convention 108 (which will be discussed in the previous paragraph). The main policy concerns of Big Data are privacy and discrimination.

4.3.1 Purpose limitation

Article 5(1)(b) GDPR sets forth the purpose limitation principle. This principle consists of a two-step test. First, the purpose for which the data is collected must be "*specified, explicit and legitimate"*. Second, if the collected data is used for further processing for any other purpose, this purpose may not be incompatible with the original purpose.[187] Article 89(1) GDPR provides an exemption to this general prohibition for further processing. Further processing for "*archiving purposes in the public interest, scientific or historical research purposes or statistical purposes*", subject to appropriate safeguards, is not considered to be incompatible with the purpose.[188] In Opinion 03/2013 on purpose limitation, the Article 29 WP has specified the meaning of the terms "*specified, explicit and legitimate"*. For a purpose to be specified, it must be sufficiently defined. This is necessary in order to enable "*the implementation of any necessary data protection safeguards"* and to set the limits of the processing operations.[189] A purpose is explicit if it is sufficiently unambiguous and clearly expressed. The notion of legitimacy provides a link with the grounds for lawful processing of Article 7 GDPR. However, legitimacy goes further than the GDPR: broader legal principles of applicable law also need to be taken into account. Furthermore, the reasonable expectations of the data subjects need to be considered.[190]

Additionally, in the DPD era the Article 29 WP provided a compatibility assessment for further processing. This assessment has been incorporated into Article 6(4) GDPR. There are some key factors that need to be taken into account among which the link between the original purpose of the collection and the purposes of the further processing.[191] But also the reasonable expectations of the data subjects, the nature of the data, the possible consequences of the further

[185] Article 5 GDPR.
[186] Article 15, 16 and 17 GDPR.
[187] Article 5(2)(b) GDPR.
[188] Art. 89(1) GDPR.
[189] Article 29 Working Party, 'Opinion 03/2013 on purpose limitation' 00569/13/EN WP 203, 2 April 2013.
[190] ibid.
[191] ibid.

processing and the existence of safeguards.[192] The Article 29 WP also addresses the issue of repurposing data for Big Data Analytics. It sets forth some safeguards that would make further use of personal data for Big Data analytics compatible. It makes a distinction between two possible scenarios of further processing.[193] In the first one, organizations make use of further processing to detect trends and correlations. Functional separation plays an important role for these analytics operations. This means that the data collected may not be used for making decisions or support measures with regard to the data subjects concerned.[194] In the second scenario, organizations try to find out information about individuals and make decisions affecting them. For this kind of use, consent would almost always be required whilst otherwise further use cannot be considered compatible with the GDPR.[195] Especially, if individuals are subject to profiling this is an important condition.

The purpose limitation principle is also established in Article 5(b) of Convention 108. The CoE Resolution (73)22 sets the requirements for this principle. According to this Resolution, the information stored needs to be "*appropriate and relevant to the purpose for which it has been stored"*.[196] Additionally, it entails a prohibition on its use "*for purposes other than those for which it has been stored.*"[197] As discussed in paragraph 3.2.2., the Big Data Guidelines have also been incorporated the principle of purpose limitation. Compared to the approach of the Article 29 WP, the Consultative Committee of Convention 108 takes a similar approach but there are some differences. E.g. the Big Data Guidelines do not require the purpose to be explicit. In my opinion, the most important contribution of the Guidelines to the CoE framework is the fact that it points out "*the transformative nature of the use of Big Data*".[198] Therefore, data controllers should identify the potential impact of the use on individuals and inform data subjects about this impact.[199] Hence, taking away some of the pressure on the principle.

Not only the GDPR and Convention 108 contain the purpose limitation principle, it is also incorporated in Article 8(2) of the EU Charter of Fundamental Rights making it one of the cornerstones of the European data protection framework.[200] Therefore, a key question that needs to be answered is what the effect of Big Data analytics on the principle of purpose limitation is? Big Data analytics often involves the use of methods and algorithms that neither the entity collecting the data, nor the data subject considered at the moment of collection.[201] However, in order to comply with the purpose limitation principle, the entity must inform the data subjects about the specific purposes of the (further) processing of their personal data. Additionally, it needs to carefully monitor its processing activities to ensure it is not exceeding the initial

[192] ibid.
[193] ibid.
[194] ibid.
[195] ibid.
[196] Committee of Ministers of the Council of Europe, 'Resolution on the protection of the privacy of individuals vis-à-vis electronic data banks in the private sector' Resolution (73)22, 26 September 1973.
[197] ibid.
[198] Consultative Committee of Convention 108, 'Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data' T-PD(2017)01, 23 January 2017 (Big Data Guidelines).
[199] ibid.
[200] Charter of Fundamental Rights of the European Union [2000] OJ C 364/1, Article 5.
[201] Zarsky (n 19).

purpose. However, this seems very hard or even impossible to realize in the field of Big Data analytics. The purpose limitation principle remains one of the core issues for data controllers. When using Big Data, it is very difficult to define the purpose of the collection and further use of the data prior to the time of collection.[202] On the one hand, Big Data analytics are challenging the purpose limitation principle. On the other hand, the principle forms a barrier to the development of Big Data analytics.[203] Inasmuch, the value of the collected data may only become apparent after it has been used multiple times for purposes other than the initial one.[204] The GDPR continues to set limits to the use of Big Data analytics, where the purpose only becomes apparent after the analysis has been completed.[205] Additionally, it is the question whether it is an effective instrument to protect individuals' rights to privacy and data protection. As mentioned before, the GDPR does provide an exception for further processing to be lawful. If the processing is conducted for "statistical purposes" it could be compatible, the extent of this exception is set out in Article 89(1) of the GDPR. According to this provision, processing for statistical purposes must be subject to "appropriate safeguards". Particularly, these safeguards must respect the principle of data minimisation by means of technical and organisational measures which may include pseudonymisation.[206] Recital 162 of the GDPR states that the result of the processing for statistical purposes may not be used "*in support of measures or decisions regarding any particular natural person."* According to some scholars, this exception seems to be difficult to apply in the context of Big Data and profiling.[207] While others (including the EU legislators) state that this exception might be a good ground for the lawful use of Big Data.[208] The GDPR has not specifically defined "statistical purposes" which means that private companies can use it for commercial gain as well. Thus, the further processing (or re-use) of personal data for Big Data applications can be lawful for "statistical purposes.[209]

4.3.2 Data minimization and storage limitation

Next, the principle of data minimization. This principle covers a wide range of aspects related to the processing of personal data. The collection of data should be limited and not excessive in relation to the purposes for which it is collected. After these purposes are fulfilled, the personal data must be removed. However, the core idea of Big Data is "*that as much data as*

[202] Nikolaus Forgó, Stefanie Hänold and Benjamin Schütze, 'The Principle of Purpose Limitation and Big Data' in Marcelo Corrales, Mark Fenwick and Nikolaus Forgó (eds), *New Technology, Big Data and the Law* (Springer Singapore 2017) <http://link.springer.com/10.1007/978-981-10-5038-1_2> accessed 10 May 2018.
[203] Information Commissioner's Office, *Big data, artificial intelligence, machine learning and data protection* (9 April 2017), Wilmslow: ICO. Available online: <https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf>
[204] Ugo Pagallo, 'The Legal Challenges of Big Data: Putting Secondary Rules First in the Field of EU Data Protection' (2017) 3 European Data Protection Law Review 36.
[205] ibid.
[206] Article 89 GDPR.
[207] Zarsky (n 19).
[208] Viktor Mayer-Schönberger and Yann Padova, 'Regime Change? Enabling Big Data through Europe's New Data Protection Regulation' [2016] The Columbia Science & Technology Law Review 315.
[209] ibid.

possible is collected and that new purposes can always be found for data already gathered."[210] It seems that the data minimization principle was not developed to prevent "*the development of massive databases or the advent of the Big Data era"*.[211] The fact that the principle of data minimization is not captured in the EU Charter of Fundamental Rights makes it easier for legislators to define its outer limits. The data minimization principle is set forth in Article 5(1)(c) GDPR. According to this principle, personal data shall be "*adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed"*.[212] In Convention 108, the data minimization principle can be found in Article 5(c). This provision states that personal data shall be "*adequate relevant and not excessive in relation to the purposes for which they are stored"*.[213] The wording of this provision connects it to the purpose limitation principle of Article 5(b) Convention 108.

Related to the principle of data minimization is the principle of storage limitation. Article 5(1)(e) GDPR and Article 5(e) Convention 108 both set forth the principle of storage limitation. The wording of these provisions is similar. This principle is meant to protect individuals from being identified longer than necessary for the purposes for which the personal data are processed.[214] Big Data analytics can result in the collection of excessive amounts of personal data that go beyond the purpose for the processing.[215] Due to the innovations in the Big Data world the volumes in which data can be stored are increasing all the time, as a result thereof the costs for storage are falling.[216] Furthermore, the ability of Big Data analytics to process these large amounts of data can result in data controllers storing historical data beyond the period necessary for normal business purposes.[217]

4.3.3 Accuracy

Article 5(1)(d) GDPR sets forth the principle of accuracy, as does Article 5(d) Convention 108. However, the principle is not incorporated in the Big Data Guidelines. Personal data needs to "*accurate and, where necessary, kept up to date"*.[218] Whenever personal data is inaccurate with regard to the purposes for which they are processed, data controllers are obligated to take "*every reasonable step*" to ensure that this data is erased or rectified without undue delay.[219] This is an important principle with regard to profiling using Big Data. The collected Big Data might entail hidden biases.[220] If the results of Big Data analytics using biased data are used to profile individuals, this could lead to erroneous predictions about the behavior of these individuals, but also, to false information about their health, creditworthiness or insurance risk.[221] Eventually,

[210] van der Sloot and van Schendel (n 29).
[211] BJ Koops, 'The Trouble with European Data Protection Law' (2014) 4 International Data Privacy Law 250.
[212] Article 5(1)(c) GDPR.
[213] Article 5(c) Convention 108.
[214] Article 5(1)(e) GDPR and Article 5(e) Convention 108.
[215] Information Commissioner's Office (n 49).
[216] ibid.
[217] ibid.
[218] Article 5(1)(d) GDPR.
[219] ibid.
[220] Information Commissioner's Office (n 49).
[221] ibid.

this could raise questions about the fairness of the processing in general. As this could have far-reaching consequence for individuals, it is of crucial importance that this principle is taken into account by data controllers using Big Data.

4.3.4 Lawful, fair and transparent processing

Article 5(1)(a) GDPR sets forth the principle of fair, lawful and transparent processing. Accordingly, "*personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject".*[222] In Convention 108, this principle can be found in Article 5(a). Individuals are afraid that Big Data analytics are a threat to their privacy, some might even find it creepy. The involvement of repurposing data in unexpected ways, the usage of complex algorithms and the drawing of conclusions about individuals with unexpected and sometimes unwelcome effects all contribute to these fears.[223] In order to guard individuals against non-transparent ways of processing the GDPR provides them with certain rights they can invoke to strengthen their legal position. For example, the data controller is obliged to provide the data subject with different sorts of information when collecting his or her personal data.[224] Moreover, data subjects have the right to obtain information about and access to information and the personal data used in processing activities concerning them.[225] New in the GDPR is the 'right to be forgotten', which gives data subjects the possibility to request the removal of all of their personal data.[226] These and other rights granted by the GDPR might help individuals to gain more insights into the Big Data analytics activities concerning them. Furthermore, the Big Data Guidelines state that in the light of the principle of transparency the conducted risk-assessments must be made publicly available. Additionally, individuals need to be informed about the potential impacts of Big Data analytics (or other uses of data) concerning them.[227]

4.3.5 Privacy by design and privacy by default

With the advances in technologies, especially the demands resulting from Big Data, the need for a proactive approach has emerged.[228] Article 25 GDPR introduces data protection by design and by default. The principle of privacy by design encourages companies and/or organizations to implement technical and organizational measures, at the beginning of the design for the processing operations.[229] It is important that these measures safeguard privacy and data protection principles from the beginning. For example, through the use of pseudonymisation

---

[222] Article 5(1)(a) GDPR.

[223] Information Commissioner's Office (n 49).

[224] Article 13 GDPR.

[225] Article 15 GDPR.

[226] Article 17 GDPR.

[227] Consultative Committee of Convention 108, 'Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data' T-PD(2017)01, 23 January 2017 (Big Data Guidelines).

[228] Ann Cavoukian and Michelle Chibba, 'Start with Privacy by Design in All Big Data Applications' in S Srinivasan (ed), *Guide to Big Data Applications*, vol 26 (Springer International Publishing 2018) <http://link.springer.com/10.1007/978-3-319-53817-4_2> accessed 10 May 2018.

[229] What does data protection 'by design' and 'by default' mean? Available online: <https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_en>

and encryption.[230] The principle of privacy by default encourages companies and/or organizations to "*ensure that personal data is processed with the highest privacy protection so that by default personal data isn't made accessible to an indefinite number of persons."*[231] For example, when creating a new Instagram account the profile settings must be set in the most privacy-friendly modus, so that the profile is not accessible to an indefinite number of persons. Section 4 of the Big Data Guidelines also entails a by-design approach, as discussed in paragraph 3.2.2.

Data protection by design and by default can be very useful instruments in a Big Data context. Privacy by design is based on the notion of building privacy features at the very beginning of the processing, which allows the early implementation of relevant controls that provide protection to individuals' personal data by default.[232] For these principles to have effect, they have to ensure the implementation of the other data protection principles.[233] As has been discussed in the previous paragraphs, Big Data analytics causes issues with multiple of the data protection principles. Therefore, data protection by design and by default also face challenges. However, the focus will be on what positive effects these principles could have on the protection of individuals.

On the basis of the four stages of Big Data analysis (as discussed in paragraph 2.3.3, the stage of data curation will be not considered here), the effectiveness of the privacy by design principle will be explained with examples. First, the stage of data collection. Data minimization is one of the core principles of data protection and, as discussed before, is under pressure with regard to Big Data.[234] By implementing specific processes that exclude unnecessary personal data from collection, reduce data fields and provide for automated deletion mechanisms data protection by design could help in enforcement of the data minimization principle.[235] Second, the stage of data analysis and curation. In this phase, anonymization methods are a good technique to preserve data inference.[236] Nonetheless, some scholars are of the opinion that anonymization is not always appropriate in all circumstances, e.g. as in the case of scientific, historical or statistical information.[237] Third, the stage of data storage. Through the use of security measures such as providing employees with limited access only and authentication are essential for protecting personal data in large databases.[238] And fourth, the stage of data usage. Here, anonymization is also a frequently used technique, e.g. for preserving privacy when data is being published.[239]

---

[230] ibid.

[231] ibid.

[232] Giuseppe D' Acquisto and others, *Privacy by Design in Big Data: An Overview of Privacy Enhancing Technologies in the Era of Big Data Analytics.* (ENISA 2015) <http://dx.publications.europa.eu/10.2824/641480>.

[233] Article 25 GDPR.

[234] D' Acquisto and others (n 232).

[235] ibid.

[236] ibid.

[237] Luca Bolognini and Camilla Bistolfi, 'Pseudonymization and Impacts of Big (Personal/Anonymous) Data Processing in the Transition from the Directive 95/46/EC to the New EU General Data Protection Regulation' (2017) 33 Computer Law & Security Review 171.

[238] D' Acquisto and others (n 232).

[239] ibid.

4.3.6 Risk-based approach

In general, people assume that the GDPR has introduced the risk-based approach to data protection. However, this is not entirely true. In 2014, the Article 29 WP published a statement "*on the role of a risk-based approach in data protection legal frameworks"*.[240] Accordingly, the risk-based approach is not a new concept, since it already existed in the DPD.[241] Especially, in Article 17 of the DPD on the security of processing and in Article 20 of the DPD on the prior checking of risks of the processing operations.[242] But also the fact that the processing of special categories is subject to stronger obligations can be seen as the application of a risk-based approach.[243] It is important to understand that a risk-based approach does not change anything about the strength of the rights of individuals, it affects the scalability of legal obligations for processing with high-risks.[244]

The GDPR contains more provisions that embrace the risk-based approach. In particular, it has been introduced as one of the core elements of the principle of accountability.[245] This is a new principle introduced by the GDPR, the principle means that "*the controller shall be responsible for and be able to demonstrate compliance with"* the other data protection principles.[246] Furthermore, it is incorporated in the obligation of the security of processing, and the obligation to carry out a data protection impact assessment (DPIA).[247] Supplemented by other implementation measures such as data protection by design[248], the obligation for documentation[249], and the use of certification and codes of conduct[250].

In the context of Big Data, the concept of a risk-based approach has been promoted in public debates. Persons in favor of the concept argue that there should be a focus shift from the collection of personal data as the main focus of regulation to legal compliance based on the framing of data use.[251] Several scholars have pointed out the shortcomings of the classic 'information-and-consent' approach to data protection.[252] For compliance, a strong harm-based approach could help in promoting responsible data use based on risk management.[253] When assessing the risk of a Big Data analysis it is important to take into account all the different

[240] Article 29 Working Party, 'Statement on the role of a risk-based approach in data protection legal frameworks' 14/EN WP 218, 30 May 2014.
[241] ibid.
[242] Article 17 and Article 20 DPD.
[243] Article 8 DPD.
[244] WP 218 (n 87).
[245] ibid.
[246] Article 5(2) GDPR.
[247] Article 32 and 35 GDPR.
[248] Article 25 GDPR.
[249] Article 30 GDPR.
[250] Article 40 and 42 GDPR.
[251] WP 218 (n 87).
[252] E.g. U. Pagallo in 'The Legal Challenges of Big Data' and F.H. Cate & V Mayer-Schönberger in 'Notice and Consent in a world of Big Data' .
[253] WP 218 (n 87).

phases of the analysis.[254] Particularly, with the pace of technological innovation privacy safeguards should be effective even before any information has been collected.[255]

4.3.7 Profiling

The provisions on profiling of both the GDPR and Convention 108 have been discussed in detail in Chapter 2. Likewise, the fact that profiling poses a threat to the fundamental rights and values of individuals has been discussed throughout paragraph 4.2. When organizations are using automated decision-making, including profiling, all of the data protection principles discussed above have to be taken into account. This is because they are both forms of automated processing and any form of automated processing is subject to the principles of Article 5 GDPR.[256] The effectiveness of the profiling provisions, therefore, depends on the effect given to the data protection framework in general. At this point, it is therefore difficult to say what the status of the provisions is. However, a Dutch scholar has made a critical assessment of the provisions on profiling in the GDPR.[257] At first sight, it seems that the GDPR is adequately regulating profiling. Article 22 GDPR has evolved to a general prohibition, and together with Article 15(1)(h) GDPR it seems to provide more protection to the dangers of profiling.[258] The threats to the right of non-discrimination are addressed by a prohibition to be subject to decisions based on solely automated processing using sensitive data (such as race and sexual preference).[259] The lack of transparency is also one of the issues posed by profiling, thus several changes have been made with regard to the right of access of the data subject.[260] This has resulted in more information obligations on the side of the data controller, and more clarity and more legal security for the data subject.[261] Furthermore, profiling could lead to false predictions and unjust correlations.[262] By stating that data controllers should adopt "*appropriate mathematical or statistical procedures for the profiling"* and implement appropriate "*technical and organizational measures"*, the risks mentioned before can be reduced.[263]

From the above, it seems that the GDPR provides sufficient protection to individuals. However, the question is whether it is enough? It seems that there are four causes that constrain its effect in practice. First of all, Article 22 and 15(1)(h) GDPR are easy to bypass. Their applicability is dependent on several conditions if one of those is not met the provisions do not apply. Van Breda sees a missed opportunity in the fact that Article 22 GDPR is not extended to

---

[254] Commissie voor de bescherming van de persoonlijk levenssfeer, *Big Data Rapport* (February 2017). Available online: <www.privacycommission.be/sites/privacycommission/files/documents/Big_Data_Rapport_2017.pdf>

[255] Pagallo (n 204).

[256] Article 4(5) GDPR.

[257] BC Van Breda, 'Profilering in de AVG: Nieuwe Regels, Voldoende Bescherming?' (2017) 154 Computerrecht 223.

[258] ibid.

[259] Article 22(4) GDPR.

[260] Article 15 GDPR.

[261] Van Breda (n 257).

[262] See paragraph 4.2.

[263] Recital 71 GDPR.

de facto automated processing with minimal human involvement.[264] Second, some grammatical ambiguities from the DPD have been copied into the GDPR. For example, the essential term "logic" of Article 15(1)(h) GDPR is not further defined by the EC.[265] Third, the GDPR provides rather broad exceptions to the general prohibition of Article 22(1) GDPR, such as the data subject's consent.[266]And finally, the effects of some valuable additions are unknown as they are only incorporated in the Recitals. This means that they do not have legal value in itself.[267] These comments provide some insight on profiling in the new GDPR, but it seems that it will take some time to figure out its exact meaning.

4.4 Added value of the Big Data Guidelines

In the Big Data era, it is difficult to maintain control over information. It is hard to understand the purpose and the way in which information is used and managed.[268] With the Big Data Guidelines, the CoE tried to move forward and describe a scenario that is different from that described in the GDPR. They may provide more challenging solutions, but they try to provide answers to the main issues that Big Data pose. The GDPR does not seem to focus on new issues such as Big Data. It mainly continues to follow the traditional approach with purpose limitation and consent as important cornerstones. Also, the GDPR entails very detailed provisions and this makes it hard to tell whether these provisions will still function in 10 years' time, although they are technology neutral.[269] The potential of the Big Data Guidelines lays with the different approach that is taken by the CoE. The main issue addressed by the Guidelines is the risk of the use of Big Data.[270] Usually, in Big Data analysis there is no focus on a specific person, so it moves beyond that, to a collective dimension.[271] By giving data controllers the obligation to consider the risk of the societal impact of the decision adopted on the basis of the Big Data analytics. It encourages a shift from individual control to a form of risk-assessment that reduces the potential negative outcomes for individuals and society.[272] Big Data makes it difficult for individuals to undertake action against processing activities concerning them. Imagine that, every time you step on your bike you have to check whether all the parts are safe or not. This is almost impossible, so is knowing what is happening to your personal data in Big Data analytics. By implementing a precautionary approach and adopting preventive policies, there is less pressure on e.g. the principles purpose limitation and data minimization.[273] However, the

[264] Van Breda (n 257).
[265] ibid.
[266] ibid.
[267] Tadas Klimas and Jurate Vaiciuk, 'The Law of Recitals in European Community Legislation' (2009) 15 Comparative Law 1.
[268] Alessandro Mantelero, 'Towards a big data regulation based on social and ethical values. The guidelines of the Council of Europe' (30 June 2017). Available online: <www.redalyc.org/jatsRepo/783/78354511006/index.html>
[269] *The GDPR & Convention 108's New Guidelines: Meeting the Challenges of Big Data* (ERA Academy of European Law) <www.youtube.com/watch?v=tenQjAxQRLM>.
[270] As is discussed in paragraph 2.2.3, the Big Data Guidelines take a risk-based approach.
[271] Mantelero (n 115).
[272] ibid.
[273] ibid.

Big Data Guidelines also have their limits. Because they are focussed on one particular technology their scope is relatively limited. Additionally, the Guidelines are not legally binding making it very difficult to enforce them by authorities.

Unfortunately, no research has been done (yet) on the implementation of these Big Data Guidelines by governments and other public or private organisations. Thus, making it difficult to determine what the actual added value of the Guidelines is. In my opinion, national data protection authorities can contribute to increasing the added value of the Guidelines. In its Fundamental Rights Report 2018, the EU Agency for Fundamental Rights (FRA) emphasises the need to identify the challenges of Big Data analytics and to find a way to address them promptly.[274] In the opinion of the FRA, EU Member States in association with their data protection authorities, should evaluate these challenges and address them "*through strong, independent and effective supervisory mechanisms"*.[275] The Big Data Guidelines could provide a good standard for the implementation of such mechanisms and so evolving into an instrument with real added value.

4.5 Recommendations

After thoroughly assessing the legal framework of the EU and the CoE together with commentaries made by legal scholars some recommendations can be made. First, the European and national data protection authorities should support organisations, both public and private, in incorporating privacy by design and privacy by default solutions for data protection issues that arise with regard to Big Data (analytics). It seems that technical and organisational measures that pursue these principles can provide effective protection to individuals. Therefore, this should be one of the priorities of these authorities. Of course, here also lies a big responsibility for the organisations themselves. When developing their Big Data analytics, these organisations should implement measures that address e.g. data minimization and data security.

Second, the European Data Protection Board should adopt an Opinion or a set of Guidelines on how to ensure compliance with the data protection principles in a Big Data context. As the previous chapters and paragraphs have shown, the traditional approach with its corresponding principles followed by the GDPR, seems difficult to apply throughout the Big Data value chain. Therefore, it would be very helpful if the EDPB would provide some guidance on how to apply the GDPR in this technology invaded era. Thus, ensuring that organisations know how to act in compliance.

And third, the CoE should try and install a committee that monitors compliance with the Big Data Guidelines. In my opinion, the Guidelines provide an excellent way of addressing the current Big Data related data protection issues. However, unlike the GDPR, they do not have a very strong position in the European legal framework. By installing a monitoring committee, the relevance of the Big Data Guidelines could get a boost.

---

[274] EU Agency for Fundamental Rights and Council of Europe, *Fundamental Rights Report 2018* (June 2018, ISBN 978-92-9491-928-1), Luxembourg: Publications Office of the European Union. Available online: <http://fra.europe.eu/en/publication/2018/fundamental-rights-report-2018>

[275] ibid.

4.6 Conclusion

Profiling and Big Data analytics threaten our fundamental rights and values. They could lead to the de-individualization of society, to privacy-intrusive commercial solicitations, to concerns related to data security and surveillance, and to hidden unfair commercial practices. Moreover, they pose risks to the right of privacy and data protection, and the right to non-discrimination. Rights that are part of the EU Charter on Fundamental Rights and Freedoms. Both Convention 108 and the GDPR are not entirely sufficient in providing a solution to these issues. Especially, the principle of purpose limitation and data minimization are threatened by the large amounts of data that are collected nowadays. However, data protection by design and by default provide a good starting point for adequately addressing the problems.

Chapter 5 – Conclusion

This thesis was aimed at assessing how the current data protection frameworks of the CoE and the EU are regulating the data protection issues posed by profiling using Big Data, and if not, recommendations would be made on how to adequately address these issues.

As depicted in the Introduction to this thesis, personal data is being collected everywhere, by everyone, all the time. These large amounts of data are known by the public as Big Data, and when used for Big Data analytics or profiling activities they could pose risks to the rights and freedoms of individuals. Big Data is usually defined using the 3V model: volume, velocity, and variety. The 3Vs refer to the amount of data processed, the speed of the data processing, and the range of data types and sources. In principle, Big Data does not have any value. In order to gain value, the data needs to go through the Big Data value chain. This chain consists of data acquisition, data analysis, data curation, data storage and data usage. Big Data analytics is the process of analysing the gathered datasets to discover patterns, inform situation and to understand and predict behaviour. The outcome of this analysis can be used for profiling purposes. Profiling is used to take decisions about individuals through the use of automated data processing techniques. Furthermore, it can be used for analysing the preferences, behaviour or attitude of specific individuals or groups of individuals. By using Big Data, the impact of the profiling can be magnified.

The rapid pace of technological developments in the last few years, decades even, asked for a change in the current regulatory data protection framework. In 2017, the Consultative Committee published a set of Big Data Guidelines trying to address the new way of collecting, combining and analysing information. The Guidelines provide a general framework of policies and measures organizations could take in order to comply with the principles and provisions of Convention 108 in a Big Data context. In 2016, the European Commission adopted the GDPR which aims at strengthening individuals' rights in an increasingly data-driven world. It introduced new obligations such as the principle of accountability and data protection by design and by default. Besides that, some of the old provisions were fortified.

Big Data analytics and profiling are increasingly putting pressure on the existing regulatory data protection frameworks. The use of these techniques could lead to breaches of the right to privacy and data protection and the right to non-discrimination. In my opinion, it would be too much to say that the current data protection frameworks of the CoE and the EU are actually failing to address today's privacy issues. However, the system has its shortcomings. The European Commission held on to the principles of purpose limitation and data minimization. These principles are put under pressure by Big Data analytics and profiling. Although the Regulation does entail a provision on privacy by design and privacy by default, these principles should have formed a larger part of the GDPR. To me, it seems that with today's technological possibilities data protection by design and by default could be of great added value to the rights of individuals. Several examples have been given on how the traditional principles are not effectively protecting them, thus examples of technological and organizational measures taken in light of privacy by design show that they provide an adequate level of protection. In my opinion, the Consultative Committee of Convention 108 took better notice of the current data protection issues by applying a risk-based approach and preventive policies. Almost daily, new scandals surrounding our privacy and data protection dominate the

news. Therefore, it is excellent that the Guidelines give a lot of attention to data controllers' obligation to take into account the social and ethical impacts of the use of Big Data.

Bibliography

Legislation

Charter of Fundamental Rights of the European Union [2000] OJ C 364/1

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (adopted 28 January 1981, entered into force 1 October 1985), ETS No. 108 (Convention 108).

Committee of Ministers of the Council of Europe, 'Recommendation on the protection of individuals with regard to automatic processing of personal data in the context of profiling' Rec(2010)13, 23 November 2010.

Committee of Ministers of the Council of Europe, 'Resolution on the protection of the privacy of individuals vis-à-vis electronic data banks in the private sector' Resolution (73)22, 26 September 1973.

Consolidated text of the modernisation proposals of Convention 108 finalised by the CAHDATA (meeting of 15-16 June 2016 (Draft Modernised Convention 108).

Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, 'Application of Convention 108 to the profiling mechanism' T-PD(2008)01, 11 January 2008.

Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281.

Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data (adopted 18 May 2018) CM/Inf(2018)15-final

Regulation (EU) 2016/679 of the European Parliament and 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) [2016] OJ L 119.

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) [2012] COM(2012)/0011.

Official documents

Ad hoc Committee on Data Protection (CAHDATA), Protocol (CETS No. 223) amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) CM(2018)2-final, 18 May 2018.

Article 29 Working Party, 'Guidelines on Automated individuals decision-making and Profiling for the purposes of Regulation 2016/679', 17/EN WP 251, 6 February 2018.

Article 29 Working Party, 'Opinion 03/2013 on purpose limitation' 00569/13/EN WP 203, 2 April 2013.

Article 29 Working Party, 'Statement on the role of a risk-based approach in data protection legal frameworks' 14/EN WP 218, 30 May 2014.

Draft Explanatory Report to the Modernised Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data [ETS No. 108].

European Data Protection Supervisor, 'Opinion 7/2015 on meeting the challenges of big data', 19 November 2015.

European Data Protection Supervisor, 'Opinion on coherent enforcement of fundamental rights in the age of big data', Opinion 8/2016, 23 September 2016.

Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS 108 (Explanatory Report to Convention 108).

Literature

Alessandro Mantelero, 'Regulating Big Data. The Guidelines of the Council of Europe in the Context of the European Data Protection Framework' (2017) 33 Computer Law and Security Review 584.

Alessandro Mantelero, 'Towards a big data regulation based on social and ethical values. The guidelines of the Council of Europe' (30 June 2017). Available online: www.redalyc.org/jatsRepo/783/78354511006/index.html

Ann Cavoukian and Michelle Chibba, 'Start with Privacy by Design in All Big Data Applications' in S Srinivasan (ed), Guide to Big Data Applications, vol 26 (Springer International Publishing 2018).

Bart Custers, 'Risicogericht toezicht, profiling en Big Data' (2014) 5 Tijdschrift voor Toezicht 9.

Bart van der Sloot and Sascha van Schendel, 'Ten Question for Future Regulation of Big Data: A Comparative and Empirical Legal Study' (2016) 7 JIPITEC 110.

Bart van der Sloot, 'A New Approach to the Right to Privacy, or How the European Court of Human Rights Embraced the Non-Domination Principle' [2017] Computer Law & Security Review.

Bart van der Sloot, 'How to Assess Privacy Violations in the Age of Big Data? Analysing the Three Different Tests Developed by the ECtHR and Adding for a Fourth One' (2015) 24 Information and Communications Technology Law 74.

Bart W Schermer, 'The Limits of Privacy in Automated Profiling and Data Mining' (2011) 27 Computer Law and Security Review 45.

BC Van Breda, 'Profilering in de AVG: Nieuwe Regels, Voldoende Bescherming?' (2017) 154

Bernard Marr, 'Why Data Minimization Is an Important Concept in the Age of Big Data' (Forbes, 16 March 2016) www.forbes.com/sites/bernardmarr/2016/03/16/why-data-minimization-is-an-important-concept-in-the-age-of-big-data/#2f3b7e31da45

BJ Koops, 'The Trouble with European Data Protection Law' (2014) 4 International Data Privacy Law 250.

Christina Tikkinen-Piri, Anna Rohunen and Jouni Markkula, 'EU General Data Protection Regulation: Changes and Implications for Personal Data Collecting Companies' [2017] Computer Law and Security Review.

Colin J Bennett and Robin M Bayley, 'Privacy Protection in the Era of "Big Data": Regulatory Challenges and Social Assessments' in Bar Van Der Sloot, Dennis Broeders and Eric Schrijvers (eds), Exploring the Boundaries of Big Data (Amsterdam University Press 2016).

Commissie voor de bescherming van de persoonlijk levenssfeer, Big Data Rapport (February 2017). Available online: www.privacycommission.be/sites/privacycommission/files/documents/Big_Data_Rapport_2017.pdf

D' Acquisto and others, Privacy by Design in Big Data: An Overview of Privacy Enhancing Technologies in the Era of Big Data Analytics. (ENISA 2015).

David Carr, 'Giving Viewers What They Want' The New York Times (24 February 2013) www.nytimes.com/2013/02/25/business/media/for-house-of-cards-using-big-data-to-guarantee-its-popularity.html?pagewanted=all&_r=0

Edward Curry, 'The Big Data Value Chain: Definitions, Concepts, and Theoretical Approaches' in José María Cavanillas, Edward Curry and Wolfgang Wahlster (eds), New Horizons for a Data-Driven Economy (Springer International Publishing 2016).

EMC Digital Universe with Research & Analysis by IDC, The Digital Universe of Opportunities: Rich Data and the Increasing Value of the Internet of Things (April 2014). Available online: www.emc.com/collateral/analyst-reports/idc-digital-universe-2014.pdf

EU Agency for Fundamental Rights and Council of Europe, *Fundamental Rights Report 2018* (June 2018, ISBN 978-92-9491-928-1), Luxembourg: Publications Office of the European Union. Available online: <http://fra.europe.eu/en/publication/2018/fundamental-rights-report-2018>

EU Agency for Fundamental Rights and Council of Europe, *Handbook on European data protection law (2018 edition)* (April 2018, ISBN 978-92-871-9849-5), Luxembourg: Publications Office of the European Union. Available online: <https://publications.europa.eu/en/publication-detail/-/publication/5b0cfa83-63f3-11e8-ab9c-01aa75ed71a1>

European Commission, The EU Data Protection Reform and Big Data Factsheet (January 2016, ISBN 978-92-79-60478-2), Luxembourg: Publications Office. Available online: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=52404

Executive Office of the President of the United States, Big Data and Differential Pricing (February 2015), Washington D.C. Available online: https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/docs/Big_Data_Report_Nonembargo_v2.pdf

Francesca Bosco and others, 'Profiling Technologies and Fundamental Rights and Values: Regulatory Challenges and Perspectives from European Data Protection Authorities' in Serge Gutwirth, Ronald Leenes and Paul de Hert (eds), Reforming European Data Protection Law, vol 20 (Springer Netherlands 2015).

Gary T Marx and Nancy Reichman, 'Routinizing the Discovery of Secrets: Computers as Informants' (1984) 27 American Behavioral Scientist 423.

Giuseppe D' Acquisto and others, Privacy by Design in Big Data: An Overview of Privacy Enhancing Technologies in the Era of Big Data Analytics. (ENISA 2015).

Hans Lammerant and Paul De Hert, 'Predictive Profiling and Its Legal Limits: Effectiveness Gone Forever' in B van der Sloot, D Broerders and E Schrijvers (eds), Exploring the boundaries of big data, vol 32 (Amsterdam University Press 2016).

Henry Pearce, 'Big Data and the Reform of the European Data Protection Framework: An Overview of Potential Concerns Associated with Proposals for Risk Management-Based Approaches to the Concept of Personal Data' (2017) 26 Information and Communications Technology Law 312, 316.

Information Commissioner's Office, Big data, artificial intelligence, machine learning and data protection (9 April 2017), Wilmslow: ICO. Available online: https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf

Ira S Rubinstein, 'Big Data: The End of Privacy or a New Beginning?' (2013) 3 International Data Privacy Law 74.

Jörg Plakiewicz, 'Convention 108 as a global privacy standard?' International Data Protection Conference (17 June 2011) https://rm.coe.int/16806b294e

Kashmir Hill, 'How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did' (Forbes, 16 February 2012) www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/#1db8bade6668

Luca Bolognini and Camilla Bistolfi, 'Pseudonymization and Impacts of Big (Personal/Anonymous) Data Processing in the Transition from the Directive 95/46/EC to the New EU General Data Protection Regulation' (2017) 33 Computer Law & Security Review 171.

Matthew Rosenberg, Nicholas Confessore and Carole Cadwalladr, 'How Trump Consultants Exploited the Facebook Data of Millions' The New York Times (17 March 2018) www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html

Mireille Hildebrandt, 'Defining Profiling: A New Type of Knowledge?' in Mireille Hildebrandt and Serge Gutwirth (eds), Profiling the European Citizen (Springer Netherlands 2008).

Nancy J King and Jay Forder, 'Data Analytics and Consumer Profiling: Finding Appropriate Privacy Principles for Discovered Data' (2016) 32 Computer Law & Security Review 696.

Nikolaus Forgó, Stefanie Hänold and Benjamin Schütze, 'The Principle of Purpose Limitation and Big Data' in Marcelo Corrales, Mark Fenwick and Nikolaus Forgó (eds), New Technology, Big Data and the Law (Springer Singapore 2017).

Omer Tene and Jules Polonetsky, 'Privacy in the Age of Big Data: A Time for Big Decisions' (2012) 64 Stanford Law Review Online 63.

Paul de Hert and Vagelis Papakonstantinou, 'The New General Data Protection Regulation: Still a Sound System for the Protection of Individuals?' (2016) 32 Computer Law & Security Review 179.

Serge Gutwirth and Mireille Hildebrandt, 'Some Caveats on Profiling' in Serge Gutwirth, Yves Poullet and Paul De Hert (eds), Data Protection in a Profiled World (Springer Netherlands 2010).

Stephanie Kirchgaessner, 'Cambridge Analytica Used Data from Facebook and Politico to Help Trump' The Guardian (26 October 2017) www.theguardian.com/technology/2017/oct/26/cambridge-analytica-used-data-from-facebook-and-politico-to-help-trump

Tadas Klimas and Jurate Vaiciuk, 'The Law of Recitals in European Community Legislation' (2009) 15 Comparative Law 1.

Tal Z Zarsky, 'Incompatible: The GDPR in the Age of Big Data' 47 Seton Hall L. Rev. 27.

The GDPR & Convention 108's New Guidelines: Meeting the Challenges of Big Data (ERA Academy of European Law) www.youtube.com/watch?v=tenQjAxQRLM

Tilman Becker, 'Big Data Usage' in José María Cavanillas, Edward Curry and Wolfgang Wahlster (eds), New Horizons for a Data-Driven Economy (Springer International Publishing 2016).

Ugo Pagallo, 'The Legal Challenges of Big Data: Putting Secondary Rules First in the Field of EU Data Protection' (2017) 3 European Data Protection Law Review 36.

Viktor Mayer-Schönberger and Yann Padova, 'Regime Change? Enabling Big Data through Europe's New Data Protection Regulation' [2016] The Columbia Science & Technology Law Review 315.

Other sources

Council of Europe, Convention 108 and Protocol: background. Available online: <www.coe.int/en/web/data-protection/background>.

Gartner IT Glossary: Big Data. Available online: <www.gartner.com/it-glossary/big-data>

Modernisation of the Data Protection "Convention 108". Available online: www.coe.int/en/web/portal/28-january-data-protection-day-factsheet?desktop=true

Strava: The Global Heatmap, Now 6x hotter. Available online: https://medium.com/strava-engineering/the-global-heatmap-now-6x-hotter-23fc01d301de

The History of the General Data Protection Regulation. Available online: https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en

What does data protection 'by design' and 'by default' mean? Available online: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_en