ARTICLE

Profiling Consumers Through Big Data Analytics: Strengths and Weaknesses of Article 22 GDPR*

Maja Nišević**

A new form of knowledge production that is flourishing in the Big Data age is profiling. In general, profiling means any form of discovering or constructing knowledge from large sets of data originating from a variety of sources. In a narrow sense, profiling is a way of making individual profiles, i.e. sets of characteristics, features, and attributes through which a person or group can be discerned from another person or group. Profiling is a relatively novel concept in European Union data protection law. It is defined in Article 4 (4) of the General Data Protection Regulation (GDPR). However, Article 22 of the GDPR determines the scope of protection in the case of profiling. This article focuses on an interpretation of Article 22. In addition, this article aims to give an overview of the wording, limitation and potential regulatory gaps, which exist in Article 22 of the GDPR.

Keywords: Big Data Analytics, algorithms, AI, GDPR, profiling, consent, contract

1 INTRODUCTION

Today, societal activities are increasingly mediated by digital technology. Digital technology gives rise to new forms of knowledge production through data analysis techniques that allow decision-making and the driving of it. The new term pointing to the growing availability of data and new data-driven practices is 'Big Data'.[1]

For sure, the age of Big Data is underway. A huge number of smartphones in every pocket, a computer in nearly every house, and an increasing number of Internet-connected devices[2] lead to rapidly increasing amounts of individuals' data that are flowing through the economy. In addition, individuals freely take part in social networks, post on blogs and send their emails on a daily basis. Today, it is equally true that individuals are increasingly monitored by companies because the data analysis is often considered as valuable to business entities and to individuals. Analysis of data can guide the prediction or the inference of the individual's preferences or behaviour. Therefore, data, particularly when collected, can reveal a lot about an individual. A new form of knowledge production that is flourishing in the Big Data age is profiling.[3] In general terms, the use of Big Data Analytics has become a tool to create individual profiles that can be used for commercial and other purposes.

In general, profiling means any form of discovering or constructing knowledge from large sets of data originating from a variety of sources.[4] In a narrow sense, profiling is a way of making individual profiles, i.e. sets of characteristics, features, and attributes through which a person or group can be discerned from another person or group.[5]

Notes

* The project leading to this application has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska -Curie grand agreement No 754345, under Region of Veneto Decree nr. 193 of 13 September 2016 and under Università degli Studi di Verona.

** Maja Nisevic is employed as the researcher at the University of Verona. Currently, she is with eLaw Institute at the University of Leiden as the visiting researcher. She is doing her Ph.D. studies at the University of Verona, and her research is focused on profiling through Big Data Analytics, considering data protection and consumer protection law. Email: maja.nisevic@univr.it.

1 Big Data is a buzzword used frequently in the private and the public domain, the press, and online media. Despite of its buzzword status and wide usage in a variety of contexts, Big Data still has no well-established definition. Most often, the variety, the velocity, and volume, commonly known as the '3-V definition', characterize Big Data. It is not clear which size datasets need to have, to label them Big Data, but Big Data obviously deals with many terabytes and petabytes. Furthermore, Big Data as buzzword is broadly applied to address a fundamental change in the way data are collected, stored, and subsequently used and all together it is a result of recent technological developments. For more *see* Abhay Kumar Bhadani & Dhanya Jothimani, *Big Data: Challenges, Opportunities and Realities Effective Big Data Management and Opportunities for Implementation* 1–24 (IGI Global 2016).

2 For example, until June 2019 in the whole world a total amount of 4,536,248,808 individuals are using the Internet connections. *See* https://www.internetworldstats.com/stats.htm.

3 *See* Paul De Hert & Hans Lammerant, *6 Predictive Profiling and Its Legal Limits: Effectiveness Gone Forever?,* Exploring the Boundaries of Big Data, vol. 32, 145–173 (2016).

4 *See* Data is power, Profiling and Automated Decision Making in the GDPR, Privacy International 2017, https://privacyinternational.org/report/1718/data-power-profiling-and-automated-decision-making-gdpr.

5 Profiling can be based on knowledge discovery in datasets (KDD) better known as data mining. Data mining refers to extracting knowledge from a large amount of data. In the other way we can say data mining is the process to discover various types of pattern that are inherited in the data and which are accurate, new and useful. It is an iterative

The first step in profiling is data processing that includes selecting, gathering data and preparing it for analysis. A second step includes analysing data through advanced processing techniques[6] in order to find patterns. Although patterns reflect correlations in the data, they are no proof of a causal relation. Therefore, the final step in profiling is the evaluation of patterns for their relevance.

In the process of profile creation, a distinction between the use of profiles in automated decision-making processes and automated decision-making based on result must be made. The use of profiles in an automated decision-making process consists of applying profiles to datasets and checking which persons, objects or phenomena conform to the profile (or generate a correlation between data with the use of algorithms).[7] In short, an automated decision-making process means construction and application of profiles by machine (e.g. computer). In this step, to make a profile, data can be used from a wide range of people. Finally, from selected patterns, a profile can be derived.[8] In this last step, it is possible to make decisions based on the result. In other words, in this last step, the application of a profile uses only the data of the persons being checked, which can be a large set or just one person. To conclude, automated decision-making based on the result is the general ability to make decisions based on the generated profiles but without human actors. Compared to profile creation, automated decision-making based on result is the process of reaching a decision based on the already created profile.[9] Furthermore, once a profile is derived, it can be used to identify people, to attribute specific risk to them, and to act upon them in specific ways.

According to Professor Custers' opinion, four types of profiling can be distinguished.[10] First, profiling as an instrument in automated decision-making based on the result, where decisions are made based on the profile without further intervention.[11] Second, profiling as a selection instrument to decide which group of person or groups deserve more attention. Third, profiling as a detection instrument to detect if certain rules have been violated, not who has violated them. Since profiling may be used for evaluating personal aspects to analyses or make predictions about individuals, the fourth type is profiling as an evaluated practice and intervention.[12]

Besides Custers' profiling types, moreover, group profiling is to be distinguished from personal profiling. In short, personal profiling concerns an individual subject or refers to the case of an individual subject being identified and targeted through a set of features.[13] On the contrary, group profiling concerns a group of individuals.[14] Considering the possibilities for all members in a group profile to share the same features, group profile may be divided into distributive and non-distributive.[15] Finally, considering the purpose of the use, profiling can be predictive or not. In a case of predictive profiling, the profile, created based on data from past behaviour or known case, is used to give inferences on future behaviour. In the end, according to Lammerant and Hert's opinion,[16] three groups are affected by the use of profiling: individuals whose data are used to create the profile, individuals to whom the profile refers, and individuals who are subject to automated decision-making based on the result (created profile).

According to Professor Savin's opinion, profiling has the potential to be harmful even if no decisions are made

Notes

process of creating a predictive and descriptive model, by uncovering previously unknown trends and patterns in vast amounts of data in order to support decision making. Data mining used two-component: first one is the database and the second one is machine learning. The origins of data mining are databases, statistics. Whereas machine learning involves the algorithm that improves automatically through experience based on data. In simple words, we can say that machine learning is a way to discover new algorithm from the experience. *See* Hert & Lammerant, *supra* n. 3 and *Data Mining V. Machine learning – Ten Best Thing You Need to Know*, https://www.educba.com/data-mining-vs-machine-learning/.

6 Big Data application means application of algorithms and machine learning on collected data.

7 *See* Mireille Hildebrandt, *Defining Profiling: A New Type of Knowledge?*, Profiling the European citizen 17–45 (Dordrecht: Springer 2008).

8 A profile does not consist of 'raw data' or mere observation. It is a mathematical model of facts or a reference to a group of facts. It should be noted that many algorithm models used for deriving profiles are opaque, because it is difficult or impossible to determine how the resulting model was built and which correlations were considered. *See* Hert & Lammerant, *supra* n. 3.

9 *See* Andrej Savin, *Profiling and Automated Decision Making in the Present and New EU Data Protection Frameworks* (7th International Conference Computers, Privacy & Data Protection 2014), https://research.cbs.dk/en/publications/profiling-and-automated-decision-making-in-the-present-and-new-eu.

10 Bart Custers, *Risicogericht Toezicht, Profiling En Big Data (Risk Based Enforcement, Profiling and Big Data)*, Risicogericht toezicht, profiling en Big Data, Tijdschrift voor Toezicht 3, 9–16 (Custers B.H.M 2014).

11 In the European Union the use of this type of profiling is restricted. The data protection law (the GDPR) forbids automated decision-making without special conditions such as 'explicitly consent' and/or 'contract performance'.

12 The use of the word 'evaluating' suggests that profiling involves some form of assessment or judgment about a person, based on which exist intervention.

13 For instance, face ID or face recognition software, as well as other forms of biometric profiling create personal profiling.

14 Once the process of data mining has established the correlation, two things happen: the construction of a category or the elaboration of a set of attributes. A category is usually called 'group' and the techniques that are used for making a category are a type of profiling based on segmentation or clustering. A set of certain attributes is called 'group profile'. It is possible that data referring to an existing group of individuals, who form some kind of community (e.g. all of them have blue eyes), are collected, aggregated, stored and processed in order to find some features. To the contrary, a category is established through the process of profiling itself and has no existence before the creation of a profile. *See* Paul & Lammerant, *supra* n. 3 and Xiaotao Gu et al., *Profiling Web Users Using Big Data*, 8(1) Soc. Network Analysis & Mining 8–24 (2018).

15 When all members share the features, the group profile is distributive. In a case of distributive profile, the individual profile can be applied to group members, because the distributive group profile gives an exact representation of the features of one individual in the group profile. To the contrary, a non-distributive profile only represents statistical relation.

16 *See* Paul & Lammerant, *supra* n. 3.

based on profiles. In particular, profiling as a technological tool introduces different levels of risk. The first risk is economical because individuals will not easily share information about themselves. A second risk is social, and it refers to the bad feeling of individuals that are being monitored by companies.[17] In any case, since profiling uses advanced processing techniques, individuals are unaware of what kind of information profiling can discover about them. Moreover, profiling itself can be very opaque, because it is based on advanced processing techniques (e.g. algorithms and machine learning).[18] Depending on what kind of algorithms is used for profiling, and how they are trained, it can be difficult for the designers of a given system to understand how or why an individual has been profiled or why the system has made a decision.[19]

From a legal perspective, it is irrelevant if profiling is part of a Big Data Analytics or not, but Big Data Analytics puts greater stress on the checks and balances in the legal framework when it comes to profiling. Further, Big Data Analytics creates a new environment in which advanced processing techniques become much more powerful. Accordingly, Big Data Analytics has changed data collection and even collection models. Since the consumer profiling means summarizing consumers data (which include their shopping habits, lifestyles, income level, preferences, demographics, and psychographics and purchase behaviour patterns), the use of Big Data Analytics has become a successful tool to create very fast consumer's profile that can be used for commercial purposes. The collection and processing of consumer's personal data through Big Data Analytics provides the possibility for traders to obtain very easily information about a consumer's preferences or expected behaviour. Information about consumers can be communicated openly to them (e.g. recommendations for a specific music show or restaurant), can be merely assumed by them (e.g. advertisement that is not obviously related to a past search), or can be hidden entirely (e.g. data being assembled and sold by data brokers, such as Acxiom, or by other third parties, as was the case in the Cambridge Analytica scandal).[20] By identifying and understanding the consumer's needs traders can use target marketing or business activities to attract the consumer to purchase products or services. For example, traders combine demographic information with data about consumer's online activities (e.g. consumer's search activity or websites visited, or posts and conversations in social media with other consumers) with an aim of focusing marketing efforts where it is most likely to get success. Moreover, consumer profile or consumer personal data are often sold to third parties (e.g. advertisers or analytical companies), which means direct monetization of personal data.[21]

When it comes to the legal framework, the relationship between profiling through Big Data Analytics and data protection must be further discussed. Consumer profiling raises questions, such as: How can consumers exercise their rights when it comes to profiling through Big Data Analytics? How do we ensure that consumer profiling is legal, fair and non-discriminatory?

Looking at the European Union legal framework, contrary to the hardly used right not to be subject to decision-making based solely on automated processing in the 1995 Data Protection Directive,[22] profiling is a relatively novel concept in the General Data Protection Regulation (GDPR). Profiling has first been regulated in Articles 4 and 22 GDPR.[23] Article 4 GDPR defines the notion of 'profiling'. However, Article 22 GDPR determines the scope of the GDPR protections in the case of profiling. Moreover, profiling has been recognized as a problem in the Article 29 Data Protection Working Party (Article 29 WP). Accordingly, Article 29 WP assumes that profiling is composed of three elements: it has to be an automated form of processing, it has to be carried out on personal data, and the objective of the profiling must be to evaluate

Notes

[17] Seventy-four per cent of Europeans desire the ability to give or refuse consent before collection or processing for online profiling purposes. *See* EU Commission, Special Eurobarometer 359, *Attitude on Data Protection and Electronic Identity in the EU* 74–75 (June 2011), http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_359_en.pdf.

[18] Profiling with use of algorithms involves a discovery phase of running large numbers of algorithms against the data to find correlations. Once relevant correlations have been identified, a new algorithm can be created and applied to cases in the application phase. The differentiation between these two phases can be regarded more simply as thinking with data and acting with data. This is a form of machine learning, since the system learns which are the relevant criteria from analysing the data. The current state of the art in machine learning is known as deep learning, which involves feeding vast quantities of data through non-linear neutral networks that classify the data based on the outputs from each successive layer. The complexity of the processing of data through such massive networks creates a 'black box' effect. This causes an inevitable opacity that makes it very difficult to understand the reasons for decisions made because of deep learning (opacity of the processing).

[19] As the Big Data Analytics leads to the finding of connections and relationships (correlations) between data that are unexpected and were previously unknown (or it is looking for the 'what', without knowing the 'why'), it is usual situation that even the designers of the system do not have answer how or why an individual has been profiled or why the system has made a decision.

[20] *See* Moritz Büchi et al., *The Chilling Effects of Algorithmic Profiling: Mapping the Issues*, Computer L. & Sec. Rev. (2019), 105367, https://doi.org/10.1016/j.clsr.2019.105367.

[21] In the literature the notion for the monetization of personal data is surveillance capitalism. Although Google learned first how to earn money by selling personal data, good illustration on the surveillance capitalists can be find in the case Cambridge Analytica. Facebook (as a social media platform) had sold personal data to Cambridge Analytica. Further, Cambridge Analytica as advertisers had used collected personal data for political advertising purposes, supported Trump's election victory and the Brexit vote. According to Prof. Zuboff, surveillance capitalism is the unilateral claiming of private human experience as free raw material for translation into behavioural data. These data are then computed and packaged as prediction products and sold into behavioural futures markets – business with a commercial interest in knowing what we will do now, soon, and later. *See* Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Profile Books 2019).

[22] *See* Art. 15 point 1 1995 Data Protection Directive.

[23] *See* Art. 4 point 4 and Art. 22 the GDPR.

personal aspects about a natural person.[24] It must, however, be taken into account that from 25 May 2018 the Article 29 WP has ceased to exist and has been replaced by the European Data Protection Board (EDPB).[25] In addition, EDPB has not issued either binding or non-binding opinions on profiling.

Considering that the GDPR is premised on deep philosophical convictions regarding the extent to which the specific rights of both individuals and groups must be protected in the digital age, it is not for surprise that the GDPR contains a more accurate and faithful expression of the various policy instruments that currently comprise the governance of privacy. A possible explanation here might be the fact that the GDPR is rooted in the traditions of EU data protection law, but it also borrows from policy innovations first introduced in countries outside Europe. Consequently, the exact scope of safeguards and rights for individuals offered by the GDPR are still the subject of some scholars' debate. Giving some examples, debates have been directed at the 'right to explanation', but also to the lack of precise language and explicit and well-defined rights and safeguards in Article 22.[26] Considering different scholars' opinions, it is not hard to conclude that the GDPR's Article 22 contains confusing wording and gaps.

Although the interpretation of the automated decision-making regulation in the Article 22 GDPR has triggered a vivid debate in the legal doctrine, the GDPR has tried to address the risks of the automated decision-making through different tool (e.g. a right to receive meaningful information about logics, significance and envisaged effects of automated decision-making; the right not to be subject to automated decision-making with several safeguards and restraints for the limited cases in which automated decisions are permitted). Accordingly, Article 22 GDPR allows an automated decision making but under wide and general conditions (i.e. contract or explicit consent or EU or Member State law). However, Article 22 directly impacts Big Data Analytics and the real challenge is to understand which safeguards could protect fundamental rights and freedoms in wide cases of consumer profiling. Consequently, this article has focused on legal analysis on the Article 22 GDPR. Since the main aim of the article is to explain the strengths and weaknesses of Article 22, when it comes to profiling, it has been divided into four Sections. After a brief introduction in this Section, section II quickly describes profiling considering Article 4 GDPR and its relevance for profiling's steps. Section III with its subsections is addressing the core problems of Article 22 GDPR. The first subsection is addressing that the wording of Article 22 is confusing. The second subsection is about exceptions in Article 22 with focus contract and consent as the main problematic exceptions offered in Article 22 GDPR. Finally, the third subsection is addressing all regulatory gaps contained in Article 22 GDPR, when it comes to profiling. Many of the points in section 3 have been made based on different scholar's opinions. However, this article highlights the central argument that confusing wording and exceptions such as consent and contract as well as regulatory gaps in Article 22 GDPR are substantial, even incurable when it comes to consumer profiling. Finally, section iv is about the conclusion.

2 Profiling and automated decision-making in the GDPR

The GDPR has introduced a new provision to address the risk arising from profiling and automated decision making. As profiling is a relatively novel concept in European Union data protection law, the GDPR defines profiling with its Article 4(4), such as:

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

In addition to Article 4 GDPR, Recital 30[27] recognizes the danger that online identifiers such as internet protocol addresses, or cookie identifiers may lead to profile creation. Considering Article 4 GDPR, profiling comprises three aspects: any form of automated processing, which means processing using computers (machine); processing that refers to personal data; the processing of personal data with the aim of evaluating personal aspects relating to an individual or group of individuals.

Notes

[24] Advice paper on essential elements of a definition and a provision on profiling within EU General Data Protection Regulation, adopted on 13 May 2013, https://www.pdpjournals.com/docs/88105.pdf.

[25] *See* https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=629492.

[26] *See* Sandra Wachter & Brent Mittelstadt, *A Right to Reasonable Inferences: Re-thinking Data Protection Law in the Age of Big Data and AI*, Colum. Bus. L. Rev. 494 (2019), https://www.law.ox.ac.uk/business-law-blog/blog/2018/10/right-reasonable-inferences-re-thinking-data-protection-law-age-big, Lokke Moerel, *Big Data Protection How to Make the Draft EU Regulation on Data Protection Future Proof*, 7–69 (14 Feb. 2014), https://pure.uvt.nl/ws/portalfiles/portal/2837675/oratie_Lokke_Moerel.pdf. Tal Z. Zarsky, *Incompatible: The GDPR in the Age of Big Data*, Seton Hall L. Rev. 47 995–1020 (2016), and Sandra Wachter, Brent Mittelstadt & Luciano Floridi, *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation*, 7(2) Int'l Data Privacy L. 77–99 (2017).

[27] Recital 30 of the GDPR: Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, particularly when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them.

As has been mentioned in the first section of this article, profiling shows three different steps. The first step in profiling is data processing that includes selecting, gathering data and preparing it for analysis (data collection). In a second step, data are analysed with the use of advanced processing techniques in order to find patterns (automated decision-making process to identify correlations). The final step in profiling is the evaluation of patterns for their relevance (automated decision-making based on result).[28] Considering the above-mentioned differences between the automated decision-making process and automated decision-making based on the result, it is clear that the GDPR in its definition does not make difference between profile creation and profile application, because its definition automatically includes analysis of data simply to predict personal preferences. Therefore, the definition in the GDPR refers just to profile creation ('any form of automated processing') and there is no requirement that the result must also be effectively applied to an individual. However, profiling means either profile creation or profile application, therefore the definition from the GDPR should contain all steps which profiling comprises.

3 How profiling is treated in Article 22 GDPR?

As the key provision for profiling, Article 22 GDPR determines the scope of the GDPR protections when it comes to profiling. However, Article 22 cannot be analysed in isolation. Its terms are defined elsewhere in the GDPR, sometimes explicitly, other times by implication. For example, Article 4(4) of the GDPR provides a definition of the notion 'profiling', but profiling must also comply with principles outlined in Article 5 and information obligation in Articles from 13 to 15.[29] Beside legally binding sources in the GDPR, a full understanding of Article 22 as a specific provision is not possible without consideration of non-legally binding sources in the GDPR. Article 22 of the GDPR should be interpreted considering Recitals from 70 to 73. In addition, as Article 29 WP issued guidance on profiling, it is welcomed to use such guidance during the interpretation of Article 22 GDPR.

Article 22 GDPR applies only in a limited set of circumstances and requirements outlined as:

> **'Automated individual decision-making, including profiling'**
>
> 1. The data subject shall have the right not to be subject to a decision based solely on automated processing, **including profiling**, which produces legal effects concerning him or her or similarly significantly affects him or her.
> 2. Paragraph 1 shall not apply if the decision:
> **(a) is necessary for entering into, or performance of, a contract** between the data subject and a data controller;
> (b) is authorized by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or
> **(c) is based on the data subject's explicit consent.**
> 3. In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.
> 4. Decisions referred to in paragraph 2 **shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) of Article 9(2)** applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

By comparing Article 22 with the definition of profiling in Article 4, it is not clear if every instance of profiling meets the definition outlined in Article 4. The definition of profiling in Article 4 requires 'any form of automated decision processing', while in Article 22 decisions have to be 'based solely on automated processing'. Moreover, Article 22 requires the decisions to produce 'a legal or similarly significant' effect on the data subject, but such requirement is not subject to the definition of profiling in the GDPR's Article 4.

3.1 *The Wording of Article 22*

Although Article 22 is a welcome development introduced by the GDPR, the wording of the provision raises numerous issues that can lead to significant misunderstandings or mistakes in the interpretation and serious gaps in the enforcement. In the following, the main wording issues will be presented and shortly discussed in order to better outline the framework for a correct interpretation of the provision

3.1.1 *Profiling as a Form of Automated Decision-Making*

From one side, heading of Article 22 ('Automated individual decision-making, including profiling') makes clear

Notes

[28] Examples of profiling include: Collection and analysis of data to gain insights into behaviours and characteristics; keeping a record of traffic violations to monitor driving habits of individuals over time to identify repeat offenders (which may have an impact on the sanction), and Considering an individual's credit score before granting a mortgage.

[29] Lukas Feiler, Nikolaus Forgo & Michaela Weigl, *The EU General Data Protection Regulation (GDPR): A Commentary* 136–137 (German Law Publishers 2018).

that profiling is a form of automated decision making. It is, however, distinct from automated decision-making, which has a broader scope.[30] From the other side, the GDPR Article 4(4) defines profiling as any form of automated processing of personal data without mentioning that profiling is a form of automated decision-making. In the literal sense of interpretation, it is not clear whether profiling alone without automated individual decision-making may give rise to safeguards under Article 22. However, it may still give rise to safeguards under Articles 13,[31] 14[32] and 15.[33] To complicate matters further, the wording in Articles from 13 to 15 ('automated decision making – including profiling') suggests that profiling is itself just a form of the decision-making process.

From the technological point of the view, profiling through Big Data Analytics is based on an automated process with the possibility to produce a significant legal effect. Until clarified by courts, it should be assumed that Article 22 covers either profiling based on any form of automated processing of personal data or profiling based on automated-decision making.

3.1.2 *The Notion of 'Data Subjects' Rights' as Referred to in Article 22*

Further, the way data subjects' rights are mentioned in the provision, opens new room for interpretation. The wording 'right not to be subject to automated-decision making, including profiling' with additional requirements,[34] can be interpreted as either 'right to object' or 'to prohibit'. From one side, if it is interpreted as a right to object, data subject could object to being subject to automated decision-making, including profiling, unless paragraph 2 of Article 22 applies. Shortly, in a case of 'contract performance' or 'explicit consent' or 'authorization of Union Member State law' data subject's right to object 'automated decision-making, including profiling' would fail. From the other side, if it is interpreted as prohibition, data controllers would not be allowed to engage automated decision-making, unless again condition under paragraph 2 of Article 22 are met. However, conditions laid down in paragraph 2 of Article 22 would have to be met before entering into a contract or performing a contract, or before getting explicit consent, or if profiling has to be authorized by Union Member State law. Considering the main aim of the GDPR,[35] Article 22, paragraph 1, should be interpreted as providing a prohibition. Therefore, data controllers can only make profiling on the data subject, if it is based on the data subject's explicit consent or if the data subject enters the contract with data controllers or performs a contract, or if profiling is authorized by law. Since profiling is based on advanced processing techniques, data subjects have a limited level of awareness in a case of profiling and cannot effectively exercise their 'right to object'. To conclude, considering that advanced processing techniques can be very complex and difficult to interpret or audit, or even explain to data subjects, Article 22(1) should be always interpreted as a prohibition even if it looks like providing a mere 'right to object'.

3.1.3 *The Notion of 'Legal' and 'Similarly Significant Effect' Produced by the Decision Based on Profiling*

Next, Article 22(1) lays out safeguards only to a decision that is 'solely based on automated processing, including profiling' and produce a 'legal' or 'similarly significant' effect on the data subject. Open questions here are: What is meant by legal or similarly significant effect? What is the nature of the effect?

Although Recital 71 of the GDPR[36] provides very limited examples of activities that would have a significant effect, from these examples it is still possible to conclude that legal or similarly significant effects are those effects that affect an individual's legal interests and rights.

In addition, it is here worth mentioning the guidelines drafted by Article 29 WP, which attempt to clarify the

Notes

[30] *See Data Is power: Profiling and Automated Decision-Making in GDPR* (Privacy International 2017), https://privacyinternational.org/report/1718/data-power-profiling-and-automated-decision-making-gdpr.

[31] Article 13: Information to be provided where personal data are collected from the data subject: (2)(f) the existence of automated decision-making, including profiling, referred to in Art. 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

[32] Article 14: Information to be provided where personal data have not been obtained from the data subject: (2)(g) the existence of automated decision-making, including profiling, referred to in Art. 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

[33] Article 15: Right of access by the data subject (1) (h) the existence of automated decision-making, including profiling, referred to in Art. 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

[34] The data subject's rights apply to decisions that are solely based on automated processing, including profiling, but Art. 22(1) requests three conditions for existence of data subject's rights. First, there must be a decision. Second, the decision has to result from automated processing and third, the decision has to result from process that includes only automated processing, without human intervention.

[35] As it is stated in Art. 1, the GDPR lays down rules relating to the protection of natural persons with regard to the processing of personal data, protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.

[36] Recital 71: '"automatic refusal of an online credit application" or "e-recruiting practices without any human intervention"'.

meaning of 'significant effect' in a much broader content than Recital 71.[37] Accordingly, Article 29 WP describes the 'significant effect' as a great or important effect and an effect that is worthy of attention. In other words, the decision must have the potential to significantly affect the circumstances, behaviour or choices of the individuals concerned; have a prolonged or permanent impact on the data subject; or at its most extreme, lead to the exclusion or discrimination of individuals. In addition, according to Article 29 WP, a legal effect requires that the decision, which is based on solely automated processing, affects someone's legal rights, and even where there is no change in data subject's legal rights or obligations. Finally, the data subject could still be impacted sufficiently to require the protections under Article 22 in case the decision produces an effect that is equivalent or similarly significant in its impact.

However, it should be noted that either Recital 71 or Article 29 WP guidelines are not legally binding. To conclude, the meaning of 'significant effect' or 'similarly effect' are both not legally mandated in the GDPR. In any case, despite the attempt by Article 29 WP and Recital 71 to describe 'significant effect' or 'similarly effect', there are still open questions: Is the burden of proof on the data subject? What are the differences between 'significant effect' and 'similarly effect' and who defines whether the data subject is vulnerable?

To complicate matters further, Article 29 WP guidelines suggest that in 'many typical cases targeted advertising does not have a significant effect on individuals'.[38] This statement is highly arguable. Exactly to the contrary, most target marketing relies on highly intrusive profiling and a clear majority of target marketing exceeds an individual's expectation. Moreover, it is equally true that most individuals primarily are just aware of the data they have shared, but not the data that are observed, inferred or predicted from their behavior.[39] Because most individuals do not even know that they are being profiled, it is becoming more difficult for them to express their wishes. Even in a case that individuals are not deprived of their freedom of choice, they can be influenced by target marketing. Finally, targeted online advertising also has the potential to lead to the exclusion or discrimination of individuals.[40] To conclude, Article 22 would also be triggered in the 'many typical cases' of the target marketing.

3.1.4 *Decisions 'Based Solely' on Automated Processing, Including Profiling*

Article 22 only applies to 'decisions' that are 'based solely' on automated processing, including profiling. Broadly speaking, the notion 'decision' covers in particular measures.[41] From the wording inside of Article 22, it is not clear whether it must be an individual decision, but the heading of Article 22 refers to an individual decision making. It can be concluded that the scope of Article 22 is limited to individual decision and profiling. From the other side the meaning of 'based solely' is not further defined in the GDPR. Adopting a literal interpretation, Article 22(1) would only refer to types of profiling excluding any human involvement altogether. In this perspective, if no human involvement at all is allowed, the scope of Article 22 would, however, be excessively small. On the other hand, there is some evidence that even where systems are explicitly intended only to support a human decision-maker, for reasons of trust in automated logic, lack of time, convenience or whatever, then the system tends to operate as wholly automated.[42] Article 29 WP defines the scope of solely automated decision-making based on profiling as automated processing in which there is no human involvement in the decision process but clarifies that the controller cannot avoid the provisions in Article 22 by fabricating human involvement and human involvement must be meaningful.[43] However, 'meaningful human intervention' is challenging to define because advanced processing techniques rely on computational algorithms, machine learning and a large amount of data. Such processing can be so complex and opaque that, as a result, those who base their decision on it, are not necessarily aware of its functions or lack the capacity to meaningful inquiry that decision. In addition, Article 29

Notes

[37] *See* Art. 29 Working Party Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, at 1–37, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053.

[38] In the guidance the following example is given: 'Women in the Brussels region aged between 25 and 35 who are likely to be interested in fashion and certain clothing items' but that example cannot be representative of current targeting practice. For instance, Facebook's Ad Targeting option alone allows the use of combinations of behaviours, demographics and geolocation data to reduce audience to one person.

[39] *See supra* n. 30.

[40] Experiments by Carnegie Mellon University showed that significantly fewer women than men were shown online ads promising them help getting jobs paying more than USD 200,000, raising questions about the fairness of targeting ads online. *See* https://www.cmu.edu/news/stories/archives/2015/july/online-ads-research.html.

[41] As it is outlined in Recital 71 sentence 1: The data subject should have the right not to be subject to a decision, **which may include a measure**, evaluating personal aspects relating to him or her which is based solely on automated processing and which produces legal effects concerning him or her or similarly significantly affects him or her, such as automatic refusal of an online credit application or e-recruiting practices without any human intervention.

[42] *See* Michael Veale & Lilian Edwards, *Clarity, Surprises, and Further Questions in the Article 29 Working Party Draft Guidance on Automated Decision-Making and Profiling*, 34(2) Computer L. & Sec. Rev. 398–404 (2018).

[43] *See Article 29 Working Party Guidelines on Automated Individual Decision Making and Profiling for the Purposes of Regulation 2016/679*, 1–37, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053.

WP's statement implies that a human being has the authority and competence to change the decision. As it has been mentioned in the first part of this article, depending on what kind of advanced technology is used for profiling, it is difficult to even for the designers of systems to understand how or why an individual has been profiled or why a system has made a decision. Therefore, strong arguments move towards extending the data subject's rights to control solely automated decision-making also to decisions made with some degree of human involvement, although the extent of that degree is hard to define and discover. According to Veale and Edwards,[44] Data Protection Impact Assessments would be the right place to assess whether a decision is indeed based on solely automated processing or not. The solution might be a document on how often a human decision-maker intervenes in decisions and whether his or her intervention changes the result of the decision at the end.

3.2 *Exceptions in Article 22*

Article 22(2) outlines three scenarios that are exceptions to the restrictions laid down in point 1: contract performance, Member State Law and explicit consent. As the GDPR not only requires the data controller to determine and specify the purpose of data collection but also to have a legal ground for the data processing,[45] therefore, Article 22(2) sets contract performance as the first possible legal ground for profiling. If this legal ground is missing, the consent of the individual must be requested. In the end, the EU Member State law could also offer legal ground for profiling.

3.2.1 *Contract*

Considering the traditional concept of contract, when two (or more) parties wish to enter into an agreement, they can conclude a contract, which will outline the rights and responsibilities of all parties. With some differences from a legal system to another, several important elements exist in a contract, including consent,[46] which represents the purest essence of the contract in every legal experience.

Considering Article 22(2) of the GDPR, profiling is permitted either if the data subject consented explicitly or is necessary for entering into or performing a contract between the data subject and the controller.[47] In the literal sense of interpretation, Article 22(2) clearly separates the notion 'consent' from the notion 'contract' even consent is an important element in a contract. From one side, it is an open question whether Article 22(2) gives the possibility for contract conclusion without consent and if not, where is the distinction between consent for contract and explicit consent. From the other side, the GDPR is silent regard to the contractual relationship between data subjects and controllers. It is not clear to what extent data subjects can perform a contract by providing personal data and how far a contractual obligation could go. Moreover, it is not even clear if the disclosure of false data (e.g. false name, age or address) can qualify as a breach of contract. Considering the guidelines Article 29 WP, there is some clarification on the notion 'necessary', but nothing is said about the formulation 'entering into, or performance of a contract' between data subject and controllers.

It seems that the notion of 'consent' should be understood as a declaration of the data subject intent, and it is not followed by the conclusion of the contract. Moreover, the European Court of Justice confirms that valid consent requires an indication of wishes.[48] Since profiling is based on any form of automated processing of personal data or on automated-decision, making valid declarations of intent (consent) under the law is 'sui iuris'.[49] Contrary, the notions 'entering into or performing a contract' should be understood as either entering into or performing the contract with a pre-formulated consent clause. To conclude, a contract is a general limitation on the use of consent as a legal basis for automated processing of personal data or automated-decision making. The conclusion of the contract with the pre-formulated consent clause automatically results in agreeing to the consent clause. Accordingly, considering the sense of the notion 'contract',[50] the data subject is one of the contractual parties in contract performance. Since the data subject is a contractual party, it is not possible to freely terminate the automated processing of personal data or automated-decision making based on a contract. If the contract is a legal basis for the profiling, termination of the contract

Notes

[44] *See* Veale, *supra* n. 42.

[45] *See* Art. 4 of the GDPR.

[46] For instance, Italian Civil Code as main condition for valid contracts requires, among others, agreement. Article 1326 of the Italian Civil Code outlines that contract is concluded in the moment when exist agreement between contractual parties. Agreement is meeting of consents between the contractual parties. Therefore, consent of the contractual parties is essential for validity of the contract. For more *see* s. 4 of the Italian Civil Code Arts 1326–1338 and Accordo contrattuale AltalexPedia, voce agg., published online on 14 Mar. 2016, written by Paolo Franceschetti, https://www.altalex.com/documents/altalexpedia/2016/03/04/accordo.

[47] *See* Art. 22 para. 2-point a and b.

[48] *See* Frederik J. Zuiderveen Borgesius *Personal Data Processing for Behavioural Targeting: Which Legal Basis?,* 5(3) Int'l Data Privacy L. 163–176 (2015).

[49] As the GPDR requires 'unambiguous' consent, request for valid consent is clear indication of wishes. For more *see* Christopher Kuner et al., *Draft Commentaries on 10 GDPR Articles (from Commentary on the EU General Data Protection Regulation*, OUP 2019) (Oxford University Press 2018).

[50] A contract is a legally binding agreement which recognizes and governs the rights and duties of the parties to the agreement and has an effect 'inter partes'.

will remove a legal basis. However, the conditions under which contracting parties are legally able to terminate a contract are defined by civil law and they are not under the scope of the GDPR. From the civil law perspective, it is still far from clear what is the nature of the contract mentioned in Article 22(2)(a). It could be understood as a contract for gift or donation or service or sales. One of the examples where profiling is followed by contract performance is a contract with a company that provides a social network site. Social network site usually offers to the data subject contract entering when opening an account but in exchange for personal data. One of the contract clauses is a pre-formulated consent clause, which allows the company to further process personal data with the aim of profiling.[51]

All things considered, it seems that Article 22(2)(a) requires an additional interpretation in the light of Member State law since it is not possible to determine the meaning of 'contract' through an isolated and independent interpretation of the concept.

Finally, it should be mentioned that some scholars believe that automated profiling does not require contract conclusion or contract performance. As a result, explicit consent of the data subject is extremely important in practice.[52] However, as it is mentioned above entering into or contract performance could be a legal basis for profiling.

3.2.2 *Consent*

Article 22(2)(c) outlines that automated-decision making, including profiling, is possible if it 'is based on the data subject's explicit consent'. However, Article 4 GDPR only defines the meaning of 'consent',[53] but is silent as to the meaning of the attribute 'explicit', which is prefixed to consent as a requirement for lawful automated-decision making, including profiling. It has been interpreted by Article 29 WP that 'explicit' consent is needed in view of the high risk of personal data processing or where a high level of individual control over personal data is considered appropriate. However, Article 29 WP does not give any indication as to when a 'high level of individual control' can be assumed to arise. Therefore, it is not clear in which cases a 'high risk' exists. Moreover, under the Recital 71[54] profiling of a child is in principle prohibited even in a case either valid consent is given by the child or valid consent is given by the holder of parental responsibility.[55]

As concerns the meaning of the definition in Article 4(11), the GDPR makes a distinction between a 'regular' and an 'explicit' consent, which means that data controllers are encouraged to use two-staged of verification of the consent. Finally, considering that Article 4(11) defines the meaning of consent for processing, a literary interpretation of Article 22(2)(c) leads to the conclusion that consent regarding profiling and consent regarding personal data processing needs to be obtained separately.

In addition, in profiling two possible situations can arise: in the first situation profiling is based on the application of a profile to an existing set of data, which have been collected with the data subject's consent; in a second situation, profiling is based instead on data, which have been collected for the explicit purpose of profiling and no previous consent about their collection exists.[56]

In the first case, in which profiling is applied to existing data, profiling itself constitutes further processing of the data. This further processing may not be incompatible with the original purposes for which the data were collected.[57]

If data are collected specifically for profiling, the controller must instead have an independent legal ground (contract) for this or the 'explicit' consent of the data subject. Typical examples where the controller has to provide consent include: using tracking/advertising cookies, sending marketing emails or newsletters, sharing personal data with other companies for profiling purposes. However, FP 7 Consent project[58] has demonstrated that individuals often give consent lightly, without properly understandings its implication. In addition, in the light of Article 7 GDPR, the data subject has a right to withdraw consent and the withdrawal of consent makes data processing unlawful from the moment of withdrawal, but not before.

Notes

[51] For example: *see* Term and services on Facebook, point 2 How our services are funded: 'Instead of paying to use Facebook and the other products and services we offer, by using the Facebook Products covered by these Terms you agree that we can show you ads that business and organizations pay us to promote on and off the Facebook Company Products. We use your personal data, such as information about your activity and interests, to show you ads that are more relevant to you', https://www.facebook.com/terms.php.

[52] *See* Lukas Feiler, Nikolaus Forgo & Michaela Weigl, *The EU General Data Protection Regulation (GDPR): A Commentary* 25 (German Law Publishers 2018).

[53] *See* Art. 4(11) 'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

[54] *See* Recital 71 of the GDPR sentence 5 'Such measure should not concern a child'.

[55] Processing of personal data shall be lawful where the child is at least sixteen years old, or if the consent is given or authorized by the holder of parental responsivity, for more *see* Art. 8 of the GDPR.

[56] *See* Lokke Moerel & Alex van der Wolk, *Big Data Analytics Under the EU General Data Protection Regulation.* This article has been first published in Dutch by SDU Uitgevers in 1–38 (2017).

[57] *See* Art. 5(1) (b).

[58] *See* https://ec.europa.eu/research/fp7/index_en.cfm.

To conclude, Article 22(2)(c) requests from a controller to bear the burden of proof that the consent is given explicitly, but the same Article does not contain more information for imposing the meaning of such consent. Considering the burden of proof, it is advisable for a controller to acquire consent from the data subject in writing. Similarly, the Court of justice of the European Union (CJEU)[59] decisions may be useful. For example, the last CJEU decision[60] is useful for a better understanding of cookie consent.[61] Shortly, CJEU made clear that tracking, marketing, and analytics cookies may only be used with explicit, clear, informed and prior consent, for example, via a consent management tool.[62] Concretely, CJEU decided that consent must be 'specific' and 'given explicitly' and in accordance with Article 13 GDPR. However, the Court did not formulate exactly the meaning of the 'explicit' consent.[63]

3.2.3 *Limitation*

Automated decision-making conducted under contracting or consenting exceptions is subject to the limitation outlined in Article 22(3). Paragraph 3 directly establishes a legal obligation for the data controller, because the data controller shall implement suitable measures to safeguard the data subject's rights. However, Paragraph 3 does not define what 'suitable measures' are, therefore, the interpretation of this notion is left to the data controllers themselves. In addition, Paragraph 3 outlines a mandatory minimum, because it states, 'at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision', which also leaves room for interpretation by the controllers.

Looking at Article 22(4) it is not possible to calculate why certain processing activities should never be allowed, because it guarantees to individuals the right not to be subject to a decision based on profiling which is based solely on automated processing of sensitive data. However, it is interesting that Article 22(4) excludes the use of sensitive data for profiling or automated decision-making on the basis of the necessity to enter into or to perform a contract.

3.3 *Regulatory Gaps in Article 22 GDPR as Regards Profiling*

3.3.1 *Right to Explanation*

Articles 13,[64] 14[65] and 15[66] GDPR require for controllers to provide information about: the 'existence of automated decision-making, including profiling', meaningful information about the logic involved and the significance and envisaged consequences of such processing, as well as the right to access to information about solely automated decision-making, including profiling. The interpretation of Articles from 13 to 15 suggests that the information for the data subject can be provided after a decision has been taken, which implies that the data subject should be able to obtain an ex-post explanation on profiling. Therefore, it is not hard to conclude that Article 22 is based on the 'right to be informed'.

However, some scholars have raised doubts about the role of the 'right to explanation' in the GDPR, arguing from the matter of fact that this right is not legally mandated in the GDPR.[67] Indeed, the 'right to explanation' is only referred to in Recital 71 of the GDPR and is, therefore, legally non-binding. Watcher, Mittelstadt, and Floridi have argued that the fact that the 'right to explanation' is not legally mandated by the GDPR represents a critical gap seriously jeopardizing transparency and accountability of profiling. Strong personal data protection requires that meaningful information should be enough to answer the question to the data subject who might force the rights to object *before* consenting to the processing and *after* the decision has been made. To conclude, the lack of a regulation concerning the ex-ante

Notes

[59] Court of Justice of the European Union.

[60] *See* Judgment in Case C-673/17 Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV v. Planet49 GmbH where the Court clarified cookie, http://curia.europa.eu/juris/liste.jsf?num=C-673/17 (Shortly, the case involved a promotional lottery, which was presented with two checkboxes: A checkbox obtaining consent for marketing emails that was not pre-ticked, but was mandatory to tick in order to participate in the lottery (Marketing Checkbox) and a pre-ticked checkbox obtaining consent to cookies, which users could opt out of at any time (Cookie Checkbox)).

[61] Cookies are files which the provider of a website stores on the website user's computer which that website provider can access again when the user visits the website on a further occasion, in order to facilitate navigation on the internet or transactions, or to access information about user behaviour.

[62] The ECJ set clear requirements on what cookie consent must look like. However, the requirements for when websites must ask for cookie consent may vary from one EU Member State to another as some Member States, such as Germany, have not implemented the Cookie Directive and the Judgment, therefore, does not apply directly.

[63] Even if the European Court of Justice confirms that valid consent requires an indication of wishes, it is however, confirms different types of a consent in different cases. For instance, the court suggests that 'consent' in Regulation (EC) No. 45/2001 requires 'express' consent (CJEU, Cases C-28/08 and T-194/04 Bavarian Lager (2010) ECLI:EU:C:2010:378, para. 77. Art. 2(h) of Regulation (EC) No. 45/2001 uses the same consent definition as the previous Data Protection Directive). In another case, the CJEU reads an opportunity to determine as requiring prior, free, specific and informed consent' (CJEU, Case C-543/09 Deutsche Telekom [2011] ECLI:EU:C:2011:279, paras 55–58). However, the case law of the court has not still explain the meaning of 'explicit' consent.

[64] *See* Art. 13(2)(f).

[65] *See* Art. 14(2)(g).

[66] *See* Art. 15(1)(h).

[67] *See* Wachter, Mittelstadt & Floridi, *supra* n. 26, at 76–99.

explanation in Article 22 GDPR entails a lack in transparency and accountability in the context of the individual's data protection, when it comes to profiling.

3.3.2 *Non-discrimination*

Non-discrimination is a consistent topic throughout the GDPR and EU law more generally,[68] however, Recital 71 outlines instructions for organizations to 'secure personal data in a manner' that will 'prevent discriminatory effect' on individuals for their membership in specific protected categories (e.g. race, political belief, religion). Therefore, as legally non-binding, Recital 71 could be assumed not legally enforceable by court.

3.3.3 *Anonymized Data*

Under Article 22 to the notion of 'data subject' assumes the definition of 'data subject' framed in Article 4(1) GDPR, as a natural person. According to this provision:

> an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Recital 30[69] made clear that profiling which uses the IP address[70] or device identifier of the user is based on pseudonymous data and the concept of profiling and pseudonymization do not exclude each other either in technical or legal sense. From the other side, this could be interpreted as if profiling did not involve the processing of data relating to identifiable natural individuals (anonymized data). Adopting this interpretation, the protection against decisions based on automated profiling would not apply to anonymized data. It must, however, be taken into account that anonymized data on their own or combined with other data are suitable to give inferences about individuals, which can be used for making decisions that have a significant effect on the individual and may impact upon an individual's behaviour or autonomy.[71]

3.3.4 *Group Profiling*

As has been mentioned in the first section, group profiling can be distributive, based on the possibilities for all members in the group profile to share the same features, without them realizing that they are members of one and the same group. However, Article 22 GDPR seems only to apply to the profiling of individual data subjects and not to the profiling of groups. Therefore, an open question is whether data subjects are protected against decisions that have a significant effect on them but are based on group profiling.

3.3.5 *Personalized Direct Marketing*

The GDPR in its Recital 70 outlines that, '"where personal data are processed for the purposes of direct marketing", the data subject should have the right to object to such processing, including profiling to the extent that it is related to such direct marketing, whether with regard to initial or further processing, at any time and free of charge'. Recital 70 is followed by Recital 71 and contains a limited description of automated individual decision-making based on profiling. It provides a number of examples, which do not include the example of profiling for the purposes of direct marketing. Further, Recital 72 outlines that profiling is subject to the rules of the GDPR governing the processing of personal data and that the EDPB should be able to issue guidance in that context. Although the legally non-binding Recital 70 offers more scope for personalized direct marketing, it seems that the GDPR does not qualify profiling for personalized direct marketing. In other words, profiling for direct marketing purposes is subject to Recital 70 and individuals 'have the right to object to receiving direct marketing'[72] including any profiling relating to such direct marketing. However, the profiling for direct marketing purposes is not subject to the provision of automated individual decision-making. From one side, it is quite true that sending direct marketing does not mean immediately a decision about an individual, because it could be based on individual perspective and do not significantly affect privacy.[73] On the other side, it may be different if profiling is used for price differentiation purposes or to exclude certain categories of individuals. In this case, the offer is not made from the

Notes

[68] *See* European Union Law Working Papers, No 31, The Meaning of the GDPR Art. 22, at 29–30 (2018).

[69] *See* Recital 30 of the GDPR.

[70] An IP address serves two-folds: host or network interface identification and location addressing, which can be used to discover the data subject. For more *see* Decision of CJEU in Case 582/14 – *Patrick Breyer v. Germany*, in which it held that IP addresses are personal data in certain circumstances, http://curia.europa.eu/juris/document/document.jsf?docid=184668&doclang=EN.

[71] Dimitra Kamarinou, Christopher Millard & Jatinder Singh, *Machine Learning with Personal Data*, Queen Mary School of Law Legal Studies Research Paper 247 (2016).

[72] *See* Moerel & van der, Wolk, *supra* n. 56.

[73] For example, sending an e-mail or displaying personalized advertising is not itself a decision about an individual, since this form of direct marketing is determined solely from the perspective of the individual.

perspective of the individual, but from the perspective of the party making the offer and it would mean a decision about individuals.

To conclude, future EDPB as it is outlined in Recital 72, should qualify personalized direct marketing as automated individual decision-making.

4 Conclusion

Profiling is a common practice in a wide variety of contexts (e.g. online advertising, health care, criminal justice). As it is demonstrated in this article, the techniques and technologies used can differ. Therefore, both profile creation and profile applications have the potential to create significant harm to individuals.

Looking at the European Union data protection law, profiling is a relatively novel concept and the GDPR attempts to regulate profiling practice. Firstly, the notion 'profiling' is defined in Article 4(4) of the GDPR. However, considering the differences between the automated decision-making process and automated decision-making based on the result, it is clear that the GDPR in its definition does not make difference between profile creation and profile application, because its definition automatically includes analysis of data simply to predict personal preferences. Secondly, Article 22 GDPR determines the scope of protection in the case of profiling. By comparing Article 22 with the definition of profiling in Article 4(4) of the GDPR, it is not clear if every instance of profiling from the Article 22 meets the definition outlined in Article 4. The definition of profiling in Article 4 requires 'any form of automated decision processing', while in Article 22 decisions have to be 'based solely on automated processing'. Moreover, Article 22 requires the decisions to produce 'a legal or similarly significant' effect on the data subject, but such requirement is not subject to the definition of profiling in the GDPR's Article 4(4). Since, automated decision-making, including profiling, can produce legal effects concerning individuals, both profile creation and profile applications should be prohibited. In addition, entering into or performing a contract, Member State law and explicit consent are conditions for legitimate automated decision-making, including profiling. However, as it is demonstrated over this article, Article 22 is either ambiguous or simply not enough defined. Firstly, the wording of Article 22 raises numerous issues that can lead to significant misunderstandings or mistakes in the interpretation and serious gaps in the enforcement. Secondly, Article 22(2)(a) requires an additional interpretation in the light of Member State law since it is not possible to determine the meaning of 'contract' through an isolated and independent interpretation of the concept. Thirdly, Article 22(2)(c) requests from a controller to bear the burden of proof that the consent is given explicitly, but either the same Article or other Articles in the GDPR does not contain more information for imposing the meaning of such consent. Finally, the GDPR's Article 22 contains regulatory gaps and the exact scope of safeguards and rights for individuals offered by the GDPR are still an open issue.