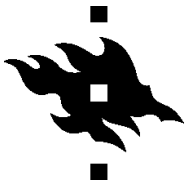

HELSINGIN YLIOPISTO
HELSINGFORS UNIVERSITET
UNIVERSITY OF HELSINKI

The GDPR, Surveillance Capitalism, AI and the personalisation of information and advertisement – A clash of ideologies and pitfalls for democracy

Master's Thesis
Author: Diana Pfau
Spring 2021
Faculty of Law
University of Helsinki
Supervisors: Ville Pönkä, Samuel Wrigley

HELSINGIN YLIOPISTO
HELSINGFORS UNIVERSITET
UNIVERSITY OF HELSINKI

Tiedekunta/Osasto - Fakultet/Sektion – Faculty		Laitos - Institution – Department
Faculty of Law		International Business Law
Tekijä - Författare – Author		
Diana Victoria Pfau		
Työn nimi - Arbetets titel – Title		
The GDPR, Surveillance Capitalism, AI and the personalisation of information and advertisement – A clash of ideologies and pitfalls for democracy		
Oppiaine - Läroämne – Subject		
Data protection Law		
Työn laji - Arbetets art – Level	Aika - Datum – Month and year	Sivumäärä - Sidoantal – Number of pages
Master	18 May 2021	80

Tiivistelmä - Referat – Abstract

Surveillance Capitalism, as described by Shoshana Zuboff, is a mutation of capitalism in which the main commodity to be traded is behavioural surplus, or personal data. As the forming of Surveillance Capitalism was significantly furthered by Artificial Intelligence (AI), AI is a central topic of the thesis. Personalisation that will oftentimes involve the use of AI tools is based on the collection of big amounts of personal data and bears several risks for data subjects.

In Chapter I, I introduce the underlying research questions: Firstly, the question which effects the use of AI in Surveillance Capitalism has on democracy in the light of personalisation of advertisement, news provision, and propaganda. Secondly, the question whether the European Data Protection Regulation (GDPR) and the Charter of Fundamental Rights of the European Union react to these effects appropriately or if there is still need for additional legislation.

In Chapter II, I determined a working definition of Artificial Intelligence. Additionally, the applicability of the GDPR together with potential problems are introduced. A special focus here lays on the underlying rationale of the GDPR. This topic is evaluated on several occasions during the thesis and reveals that the focus of the GDPR on enabling the data subject to exercise control over his or her information conflicts with the underlying rationale of Surveillance Capitalism.

In Chapter III, four steps of examination follow. In a first step,I introduce the concept of Surveillance Capitalism. Personalized advertisement together with consent as a legal basis for processing of personal data are examined. During this examination, profiling, inferences, and the data processing principles of the GDPR are explored in the context of personalisation and AI. A focus in this examination is the question how individuals and democracy can be impacted. It is found that there is a lack of protection when it comes to the use of consent as a legal basis for privacy intrusive personalized advertisement and it is likely that the data subject will not be able to make an informed decision when asked for consent. Data minimisation, purpose limitation and storage limitation as important data processing principles proof to be at odds with the application of Artificial intelligence in the context of personalisation. Especially when it comes to the deletion of data further research in AI will be necessary to enable the adherence to the storage limitation.In a second step, I examined personalized news and propaganda according to their potential impacts on individuals and democracy. Explicit consent as a legal basis for processing of special categories is examined together with the concept of data protection by design as stipulated in article 25 GDPR. While explicit consent is found to likely suffer from the same weaknesses as the “regular consent”, I proposed that data protection by design could solve some of the arising issues if the norm is strengthened in the future.In a third step, I evaluate whether the right to receive and impart information laid down in the Charter of Fundamental Rights of the European Union provides for a right to receive unbiased, or unpersonalized, information. While there are indications that such a right could be acknowledged however, its scope is unclear so far. In a fourth step, I examine the proposal for a European Artificial Intelligence Act with the unfortunate outcome, that this Act might not be able to fill the discovered gaps left by the GDPR.

I conclude that, taking into consideration all findings of the research, the use of AI in personalisation can significantly harm democracy by potentially impacting the freedom of political discourse, provoking social inequalities, and influencing legislation and science through heavy investment and lobbying. Ultimately, the GDPR does leave

significant gaps due to the incompatibility of underlying rationales of the GDPR and Surveillance Capitalism and there is a need to protect data subjects additionally. I propose that future legislations on the use of AI in personalization should react appropriately to the rationale of Surveillance Capitalism.

Avainsanat – Nyckelord – Keywords
European Data Protection Law, Surveillance Capitalism, Democracy, Privacy

Säilytyspaikka – Förvaringställe – Where deposited

E-thesis Helsinki University

Muita tietoja – Övriga uppgifter – Additional information

List of Abbreviations

Artificial Intelligence (AI)

Charter of Fundamental Rights of the European Union (Charter)

Court of Justice of the European Union (CJEU)

European Court of Human Rights (ECtHR)

European General Data Protection Regulation (GDPR)

Content

I. Introduction

Recently, the United Nations Secretary General Antonio Guterres called for international cooperation in battling the spread of white supremacy, propaganda, and disinformation. He also explicitly referred to the use of social media contributing to the absence of facts in news provision.[1]

Similarly, prominent figures like Elon Musk, Stephen Hawking, Bill Gates and Steve Wozniak published an open letter in 2015 warning of the revolutionary nature of Artificial Intelligence (AI).[2] The letter, by now signed by over 8000 people, praises the potential of AI, while warning that the magnification of human intelligence by AI tools has the potential for great pitfalls and therefore it will be important to research how to reap its benefits.[3] Interestingly, in the enclosed research proposals of this letter, the long-term research objectives mentioned include not only validity and security, but also the idea that even if general AI will become reality one day, meaningful human control must be ensured.[4]

The fact that leading figures in the field acknowledge that AI does not only have potential to lead to the benefit of people, but also carries enhanced dangers, is significant. Critically, the "discovery" of AI did also significantly contribute to the development of Surveillance Capitalism. It is to say here, that the perception of Surveillance Capitalism as a technological necessity is to be rejected.[5] Nevertheless, AI and big data played an important role in the

---

[1] Al Jazeera, "UN chief urges global alliance to counter rise of neo-Nazis" (26 January 2021) <https://www.aljazeera.com/news/2021/1/26/un-chief-urges-global-alliance-to-counter-rise-of-neo-nazis>, last accessed 28 January 2021

[2] Leopold Schmertzing, "Democracy in the Age of Artificial intelligence" in Danièle Réchard (ed) *Global Trendometer, Essays on medium- and long-term global trends July 2018* (European Parliamentary Research Service, Essays on medium- and longterm global trends, 2018) 17

[3] Research Priorities for Robust and Beneficial Artificial Intelligence <https://futureoflife.org/ai-open-letter/?cn-reloaded=1>, last accessed 22 December 2020

[4] Stuart Russell, Daniel Dewey, Max Tegmark, "Research Priorities for Robust and Beneficial Artificial Intelligence" [2015], <https://futureoflife.org/data/documents/research_priorities.pdf?x96845>, last accessed 10 December 2020

[5] Shoshana Zuboff, *The Age of Surveillance Capitalism- the Fight for a human future at the new Frontier of Power* (Profile Books, 2019) 15

forming of Surveillance Capitalism and its further development and application. This mutation of capitalism, described as a change of the logic of accumulation[6] from goods and services to data (or behavioural surplus[7]), carries many potential problems not only for individuals but also on a societal level. Surveillance Capitalism strives for asymmetries of knowledge and power while translating whole lives into data that is to be expropriated and repurposed into new forms of social control, oftentimes without the data subjects' knowledge.[8] The logic of Surveillance Capitalism as proposed by Shoshona Zuboff will be examined and applied in the following chapters also to understand whether the European General Data Protection Regulation (GDPR)[9] can be successful in governing these surveillance measures by companies.

Phenomena resulting from the use of new technologies that can be seen already nowadays are manifold. A first point to mention is a dying printed press industry due to news provision by means of social media instead of traditional journalism. [10] Secondly, social media are now able to influence elections and their results. [11] I[12] propose that both of these developments are highly connected with the use of AI in personalisation. The use of AI enhances the capabilities of data analysis and decision-making. Thirdly, there is an ever-growing amount of (personal) data being created and traded.[13]

---

[6] Shoshana Zuboff, *The Age of Surveillance Capitalism- the Fight for a human future at the new Frontier of Power* (Profile Books, 2019) 52-54
[7] ibid 8.
[8] ibid 54-55.
[9] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1
[10] Paul Niemitz, "Constitutional democracy and technology in the age of Artificial Intelligence" [2018] Phil.Trans.R. Soc. 1, 6
[11] Ibid.
[12] The use of the first person here is made out of conscious choice as the thesis displays original work and opinions of the author.
[13] Lilian Mitrou, "Data Protection, Artificial Intelligence and Cognitive Services- Is the General Data Protection Regulation (GDPR) 'Artificial Intelligence-Proof?'" [2019] <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3386914> last accessed 10 December 2020, 1, 8

As data collection is in the centre of Surveillance Capitalism, the focus in the following will lay on personalisation in advertisement and in news provision since personalisation utilizes a lot of data. The personalisation of news will be examined due to the crucial role of news provision in political participation of citizens to ensure a working democracy. Democracy is not a static situation, but a state that constantly must be realized.[14] To understand potential benefits and risks for democracy, I will firstly examine the definition of AI.

Then, I will introduce the GDPR together with potential problems arising with the treatment of AI in Surveillance Capitalism. The GDPR will be the main legal body that will be examined in the following, as it is a central legal instrument for protection of personal data within the European Union and had an impact on data protection laws worldwide. I will then examine personalized advertisement together with consent as a legal ground for processing of personal data and several of the principles of processing laid down in the GDPR. Subsequently, personalized news provision and propaganda will be explored together with the protection given by the GDPR when it comes to special categories of data. Further, I will consider the possibility of a right to unbiased information under the Charter of Fundamental Rights of the European Union (Charter).

Lastly, I will give an outlook on the proposed AI regulation and answer the research questions.

1. Research Questions

The research questions that will be examined in the following, are firstly: What are the effects of AI and Surveillance Capitalism on democracy when it comes to personalisation of advertisement, news provision, and propaganda? And secondly: How do the GDPR and the Charter react to these effects and is there still need for additional legislation?

---

[14] Christian Djeffal, "AI, Democracy and the Law", in Andreas Sudmann (ed), *The Democratization of Artificial Intelligence- Net Politcs in the Era of Learning Algorithms* (transcript Verlag, 2019), 255, 260

I consider research in this field as beneficial and indeed necessary for several reasons. AI brings about many changes and developments in the field of technology. The focus of companies and market participants now lays on an unprecedented collection of behavioural data to be traded and used for predictions about individuals and their future behaviour.[15] Shoshana Zuboff goes as far as arguing that this marks a new form of information capitalism.[16] While AI is not the cause for this focus on data, it describes a whole field of new technologies that improve the capabilities for companies to collect and use data and is therefore strongly connected to the forming of Surveillance Capitalism. It is important to evaluate the potential consequences of the current and future use of AI for the individual, society, and democracy as a whole for several reasons.

AI will oftentimes be used when it comes to personalisation of advertisement and news provision. [17] This means that AI also has direct influence on individuals and the potential to have direct influence on individuals' information regarding certain topics. This individual dimension of AI is addressed also in the GDPR, but the question will arise whether the GDPR grasps AI in a manner that the data subject is sufficiently protected.

Additionally, AI can also have an impact on societies. Questions of justice, fairness and distributive fairness arise when being confronted with personalisation and decisions coming with it.

Moreover, it is to acknowledge that the field of research on AI is widely dominated by only a few powerful actors.[18] Questions of power over the development of this field of technology arise and must be examined. This will be especially important when one raises the question how and according to which criteria the technology is developed. It will be necessary to also think

---

[15] Shoshana Zuboff, *The Age of Surveillance Capitalism- the Fight for a human future at the new Frontier of Power* (Profile Books, 2019) 8
[16] ibid 12.
[17] Frédéric Marty, Thierry Warin, "The use of AI by Online Intermediation Platforms Conciliating Economic Efficiency and ethical Issues" (2019) 4 Delphi 217, 217
[18] Paul Niemitz, "Constitutional democracy and technology in the age of Artificial Intelligence" [2018] Phil.Trans.R. Soc. 1, 3-4

about the desirability of the outcome of this development of technology ultimately regarding individuals, societies, democracy, economic markets, and legislators.

Lastly it is to say, that research on this topic is important now because the field of AI is still not fully developed and there is room for asking questions and influencing the development in a way that benefits democracy.

2. Methodology

I will attempt to answer these question by using a socio-legal methodology. This is to gain a better understanding of the matter by examining the law in the context of the environment in which it operates. Social, individual, and technological consequences and circumstances will therefore be taken into account. The socio-legal methodology enables this approach and allows for interdisciplinary or multidisciplinary approaches.[19] In doing so, legal scholars are to familiarize themselves with methodologies and literature in related fields.[20] Socio-legal research is defined by not only investigating the field of law, but it encompasses a range of perspectives and methodologies.[21] Within this research, law is not seen as an abstract and closed system in itself. Law is a social product and cannot be fully understood without understanding its surrounding circumstances. Social circumstances are understood to infuse the meaning of, and shape, the law.[22]

Even though the name suggests that this type of research would only focus on law in a societal context, it goes far beyond this. This research has an inherently trans- or interdisciplinary character and provides the possibility to connect legal research to other disciplines.[23]

---

[19] Nicole Graham, Margaret Davies, Lee Godden, "Broadening law´s context: materiality in socio-legal research" (2017) 26 Griffith Law Review 481, 501
[20] ibid.
[21] ibid 482.
[22] Nicole Graham, Margaret Davies, Lee Godden, "Broadening law´s context: materiality in socio-legal research" (2017) 26 Griffith Law Review 481, 484.
[23] ibid 501.

In this paper, I will borrow ideas from various fields. Not only will I discuss questions of technology in examining AI, I will also reflect on political, economic, social, and philosophical concepts briefly and how they might influence, or be influenced by, law. This approach seems justified as the question how democracy can be impacted or influenced by technology is a topic that necessarily needs to include questions of how the law should be, which values one finds within a society and also why certain laws are the way they are now.

II. Artificial intelligence and applicability of the GDPR

In the following, I will find a working definition of AI for this paper and give a short overview over the applicability of the GDPR when it comes to AI and challenges that can arise in connection to the GDPR.

1. AI definition and problems arising

To understand the effects that the use of AI has on democracy and individual users, it is necessary to gain an understanding of what AI is first. It is to mention however that AI truly is not a clear-cut technology but rather inspired the development of a whole strain of computer science and therefore stands out in its openness.[24]

To start with the basics, it is important to define the basis of AI: Algorithms. An algorithm can be simply defined as "a finite set of rules which gives a sequence of operations for solving a specific type of problem".[25] An algorithm will typically be used to perform a certain task that can vary from printing a certain statement such as "Hello World" to performing a numerical calculation. Algorithmic systems are also meant to perform a specific task that can be more complex, like the anticipation of the outcome of a certain decision, or the detection or classification of something unknown by using inferences rather than a direct measurement.[26]

Artificial Intelligence is based on algorithms. When it comes to defining AI, there is no definition of the term that is agreed upon.[27] Some of the definitions are based on the idea of "intelligence" which is defined in various ways.

---

[24] Christian Djeffal, "AI, Democracy and the Law" in Andreas Sudmann (ed), *The Democratization of Artifcial Intelligence- Net Politcs in the Era of Learning Algorithms* (transcript Verlag, 2019), 255, 257

[25] Donald E. Knuth, *Fundamental Algorithms- The Art of Computer Programming* (2nd edn, Addison -Wesley Publishing Company, 1973) 4

[26] Lilian Edwards and Michael Veale, "Slave to the Algorithm? Why a 'Right to an Explanation' is probably not the remedy you are looking for" (2017) 16 (1) Duke Law and Technology Review 18, 24

[27] Christian Djeffal, "AI, Democracy and the Law", in Andreas Sudmann (ed), *The Democratization of Artifcial Intelligence- Net Politcs in the Era of Learning Algorithms* (transcript Verlag, 2019), 255, 256

The first attempt to define intelligent machines stems from 1950 and came from Alan Turing. For him a machine can be deemed intelligent if it can engage in a text conversation that would fool a human into thinking the machine was also a human.[28] This definition seems to be outdated for defining "intelligence" in "Artificial Intelligence" nowadays as AI already developed past a mere text conversation and already reached a point where voice conversation is possible. This definition would exclude new AI methods and narrow the field of AI without an apparent necessity to do so. Rather, I propose to not change the scope of what is considered to be AI for the purposes of this paper and therefore, I reject this definition.

Five years later John McCarthy, the so-called father of AI,[29] defined intelligence in machines as a behaviour of a machine or the performing of a task by a machine that would require intelligence when performed by a human.[30] This definition, however, seems to be disputable as well. Instead of finding a definition of intelligence, rather McCarthy simply referred to another form of intelligence that is just as unclear as the originally disputed term.

The problem of defining "intelligence" remains. One example of that is the European AI Strategy definition of AI that defines Artificial Intelligence as follows: "Artificial intelligence refers to systems that display intelligent behaviour by analysing their environment and taking action, with some degree of autonomy, to achieve specific goals".[31]

---

[28] Dimitra Kamarinou, Christopher Millar, Jatinder Singh, "Machine learning with personal data" (Queen Mary University of London, School of Law, Legal Studies Research Paper 247/2016) 1, 3

[29] Andy Peart, "Homage to John McCarthy, the father of Artificial Intelligence (AI)" [2020], <https://www.artificial-solutions.com/blog/homage-to-john-mccarthy-the-father-of-artificial-intelligence>, last accessed 4 November 2020

[30] Dimitra Kamarinou, Christopher Millar, Jatinder Singh, "Machine learning with personal data" (Queen Mary University of London, School of Law, Legal Studies Research Paper 247/2016) 1, 3

[31] S Samoili et al., "AI Watch Defining Artificial Intelligence Towards an operational definition and taxonomy of artificial intelligence" (Publications Office of the European Union 2020) 9

While Turing and McCarthy referred to human intelligence to compare the performance of a machine with the performance or acceptance of a human being, later authors took other approaches. They referred to intelligence as a form of rationality,[32] or come back to a certain performance, such as problem solving capability coming with intelligence,[33] or even a reconstruction of the human brain and therefore an artificial reproduction of the human intelligence.[34]

I question the comparison that is drawn between human intelligence and machine intelligence. Human intelligence itself is a rather disputed field within literature and lacks a uniform definition. Britannica defines human intelligence as the "mental quality that consists of the abilities to learn from experience, adapt to new situations, understand and handle abstract concepts, and use knowledge to manipulate one's environment"[35]. While it seems intuitively comprehensible to recourse to intelligence as a concept when thinking of Artificial Intelligence, it can also be misleading. In fact, relying on human intelligence for defining purposes, can lead to false worries and expectations and should therefore be rejected here.

Additionally, the reliance on human intelligence for definition purposes would for example exclude the current technologies that are seen to be AI from the definition as the general AI, that would be conscious or intelligent comparable to a human being does not exist so far.[36] In fact, one can only guess whether the development will lead to general AI. This means, that AI nowadays can perform certain tasks professionally, or intelligent, but cannot interact with the world and manipulate its environment in a way a human being would. To draw a realistic picture therefore, in the following a

---

[32] Pei Wang, "On Defining Artificial Intelligence" [2019] Journal of Artificial General intelligence 1, 19
[33] ibid 10.
[34] ibid 8.
[35] Robert J. Sternberg, "Human intelligence", <https://www.britannica.com/science/human-intelligence-psychology>, last accessed 4 November 2020
[36] Lilian Mitrou, "Data Protection, Artificial Intelligence and Cognitive Services- Is the General Data Protection Regulation (GDPR) 'Artificial Intelligence-Proof?'" [2019] < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3386914> last accessed 10 December 2020, 1, 11

definition will be favoured that departs from the idea of human intelligence and rather focuses on main properties of AI to avoid unnecessary confusion and to give a realistic picture about what AI is able to achieve. This approach is favoured also to ensure that the legal discussion focuses on the properties of AI models rather than on abstract questions of consciousness of AI or similar.

One property of AI is the ability to learn from experience, meaning that AI can learn from patterns detected in data sets.[37] Machine learning is an important approach to achieve AI.[38] It is defined as any methodology or set of techniques that are designed to find novel patterns and knowledge in data and generate models that can be used for effective predictions about certain data.[39] Machine learning algorithms are probabilistic, i.e. their output changes according to the learning dataset that is fed into the algorithm.[40]

There are several ways of learning that can be applied nowadays: Supervised, unsupervised, and reinforced learning. An interesting property lays in the fact that for example unsupervised learning works without labelling or correct outputs. What the AI model is trained to do is to discover the structure of a data set.[41] The learning process therefore is not a controlled and rulebased approach, but rather depends on a feedback loop. Importantly, this will influence questions of the implementation of certain rules into the design and should be kept in mind when thinking of a logic structure of approaching AI also from a legal point of view. Evidently, this already reveals a high

---

[37] Lilian Mitrou, "Data Protection, Artificial Intelligence and Cognitive Services- Is the General Data Protection Regulation (GDPR) 'Artificial Intelligence-Proof?'" [2019] < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3386914> last accessed 10 December 2020, 1, 10
[38] ibid 12.
[39] ibid.
[40] ibid 13.
[41] Sanatan Mishra, "Unsupervised learning and Data Clustering" [2017]) <https://towardsdatascience.com/unsupervised-learning-and-data-clustering-eeecb78b422a> last accessed 5 February 2021

dependence of AI applications on data[42] not only in a quantitative dimension but also qualitatively to achieve accuracy.[43]

Another characteristic of AI that must be considered, is AI tools' unpredictability. This means, that one is unable to predict what specific actions AI precisely and consistently will take to achieve the given objective even if the terminal goals of the system are known.[44] This also means that one might not be aware beforehand which data and detected pattern in the given data is taken into account when coming to a certain prediction. Critically, it will have to be considered how this unpredictability will influence the implementation of data protection principles as mentioned in the GDPR and also raise questions on how this influences, or should influence, the treatment and safeguards of inferences that can be drawn and used by AI.

I therefore propose the following definition: Algorithmic systems that can perform either a limited amount or a wide range of tasks professionally and with an element of "surprise" or unpredictability stemming from self-optimization through a process of learning from data. AI is reinforced by other developments and trends and should be seen within the context of a shift in how we perceive and use technology nowadays. This paper, this definition will be used to understand the basic idea of AI.

It is to mention, that the definition is not exhaustive and can clearly be disputed. Important for the following is however, to have a realistic picture about AI. AI is a wide field that includes many technologies that are still under development. The most important points to remember however are, that there is a learning process from data, that there will oftentimes be a large amount

---

[42] Dimitra Kamarinou, Christopher Millar, Jatinder Singh, "Machine learning with personal data" (Queen Mary University of London, School of Law, Legal Studies Research Paper 247/2016) 1, 14

[43] Lilian Mitrou, "Data Protection, Artificial Intelligence and Cognitive Services- Is the General Data Protection Regulation (GDPR) 'Artificial Intelligence-Proof?'" [2019] <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3386914> last accessed 10 December 2020, 1, 26

[44] Roman V. Yampolskiy, "Unpredictability of AI: On the impossibility of Accurately Predicting All Actions of A Smarter Agent" (2020) 7 Journal of Artificial Intelligence and Consciousness 109, 110

of data collected and used to optimize predictions, and that the current state of technology is a narrow AI that can only perform a limited amount of tasks professionally.[45]

2. The GDPR and its applicability to AI

The European General Data Protection Regulation or GDPR, entered into force in 25 May 2018 and is an important tool for data protection not only within Europe, but influenced Data Protection laws all over the world.[46] As the GDPR is oftentimes celebrated as the most developed regulation in the field of data protection law, I will focus on this regulation mostly.

As the underlying idea of data protection laws, is the protection of privacy, I will firstly examine the idea of privacy. There are many different definitions of privacy as underlying rationale for data protection laws. Privacy can be regarded as a general right to not be subject to interferences from the outside.[47] It can also be defined as the degree of access to a person.[48] Lastly, privacy can be defined as the right to information control. In this approach the data subject is seen to have the right to determine when, how and to what extend information about them is revealed or communicated to others.[49] The perception of privacy as the right to informational control is the most common in data protection discourse.[50] The GDPR also seems to cite with this definition as it explicitly refers to the necessity that the data subject should have control over his or her personal data.[51] Values that further the aim of privacy are, among others, individuality, autonomy, dignity, integrity, and

---

[45] Lilian Mitrou, "Data Protection, Artificial Intelligence and Cognitive Services- Is the General Data Protection Regulation (GDPR) 'Artificial Intelligence-Proof?'" [2019] <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3386914> last accessed 10 December 2020, 1, 10-11

[46] Ben Wolford, "What is GDPR, the EU's new data protection law?" <https://gdpr.eu/what-is-gdpr/> last accessed 10 May 2021

[47] Lee A. Bygrave, *Data Protection Law, Approaching its Rationale, Logic, and Limits,* (Kluwer Law international, 2002) 128

[48] ibid.

[49] ibid 129.

[50] ibid 130.

[51] Recital 7 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1

self-evaluation.[52] All of these values are to enhance the individual's capability and space for self-realization.[53] These concepts are important when thinking of whether the GDPR does provide adequate protection for the data subject.

While in the following the GDPR will be assessed according to its applicability to AI, it is to note that the text of the GDPR, out of conscious choice, is technology neutral.[54] This is because law, as opposed to technology, reacts slowly. The procedure of negotiating, agreeing, and enacting new laws within the European Union is a lengthy process. Therefore, it cannot be expected that law can react to new technologies as well as new possible problems in time. The choice of technological neutrality hence seems to make sense as the principles laid down will be applicable to any type of processing and include new, unexpected developments.[55]

This statement however will not necessarily stay true. The neutrality leads to a certain extent of vagueness in the GDPR. It is yet to be seen whether legal certainty will be achievable in the long run, or if the vagueness will lead to legal uncertainty and therefore impact the protection of data subjects´ rights.[56] This would also mean that the applicability of the GDPR might be circumvented for certain technologies in the future. In fact, unexpected developments have the potential to, even if they are covered by the GDPR somehow, raise new problems that the drafters of the GDPR did not necessarily think of and that would require new legislation.

---

[52] Lee A. Bygrave, *Data Protection Law, Approaching its Rationale, Logic, and Limits,* (Kluwer Law international, 2002) 133-134
[53] ibid 134.
[54] Recital 15 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1
[55] Lilian Mitrou, "Data Protection, Artificial Intelligence and Cognitive Services- Is the General Data Protection Regulation (GDPR) 'Artificial Intelligence-Proof?'" [2019] <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3386914> last accessed 10 December 2020, 1, 26
[56] ibid 27.

When it comes to the use of AI and related technologies, such as machine learning and big data that are undeniably strongly interconnected with AI,[57] the GDPR gives rise to many concerns. EU policy makers made clear that the GDPR shall help enhancing big data analysis by contributing to trust and therefore lead to greater employment and contribution from data subjects.[58] This statement itself is already contestable.

Trust is not the same as actual protection of data subjects and respect of their privacy. In fact, the recitals of the GDPR seem to oftentimes lay the focus on the functioning of the internal market, rather than on privacy or protection of data subjects. Recital 13 of the GDPR for example states that "the proper functioning of the internal market requires that free movement of personal data within the Union is not restricted or prohibited for reasons connected with the protection of natural personals with regard to the processing of personal data". This seems to be in significant contrast to the actual title of the GDPR that clearly mentions "the protection of natural persons with regard to the processing of personal data" and the "free movement of such data". It can be seen here that the GDPR strives for finding a balance between the protection of personal data and the free movement of data and therefore its commercial use.

While it is not disputed that the GDPR does give a wide catalogue of rights to the data subject, it has to be questioned in how far the GDPR does indeed "help" the data subject. In fact, this seems to reflect the nature of data protection laws in general. While one is oftentimes tempted to think that laws for data protection are in fact to protect one´s privacy only, they are nothing but a legal guidance for which and how much of this data can be used for economic or other purposes.

---

[57] S Samoili et al., "AI Watch Defining Artificial Intelligence Towards an operational definition and taxonomy of artificial intelligence" (Publications Office of the European Union 2020) 12

[58] Recital 7 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1

I propose, that the very economic nature of data nowadays and the focus of data protection laws on the free flow of data generally run the risk of a lack of protection of privacy. Especially when focusing on the control over personal data for the data subject, there is reason to believe that the GDPR, as the main focus of this paper, is not prepared for the age of Surveillance Capitalism in which data is traded often without the knowledge and understanding of the data subject.[59]

One line of questions that can arise is also whether this undue emphasis on the internal market is the expression of powerful mega corporations lobbying for their cause. It is also disputable whether the wealth that is created by operations including extensive data use is reaching societies or not.

Another problem that will be addressed in the following is the data processing principles in article 5 GDPR. It was argued that data minimization is in contrast with the use of big data and AI. [60] Similar was argued for the purpose limitation.[61] This view however seems to neglect the fact that AI is still in the development phase in many regards. This means that there is still room for AI to be developed in a way to adhere to these principles. Therefore, the principles might lead to changes in the way AI is designed and lead to benefits for both the controller, as the entity determining the means and purposes of processing,[62] and the data subject. This, however, will be dependent on the actual incentive given to controllers and the feasibility to change the way AI is designed.

To sum up shortly the GDPR is applicable to AI. However, the technological neutrality in the GDPR, even though it could be beneficial in the sense that it does not harm the GDPR's applicability to new technology, might also lead

---

[59] Shoshana Zuboff, *The Age of Surveillance Capitalism- the Fight for a human future at the new Frontier of Power* (Profile Books, 2019), 11

[60] Tal Z. Zarsky, "Incompatible: The GDPR in the Age of Big Data" (2017) 47 Seton Hall Law Review 995, 1010

[61] ibid 1007.

[62] Article 4(7) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1

to legal uncertainty and give rise to problems. The text of the GDPR is also oriented on drawing a balance between the rights of data subjects and the free flow of personal data and it can be questioned, if this balance is always found. In line with this comes also the question whether the GDPR is able to establish a concept in which the distribution of wealth comes back to the data subjects, or if distributive fairness cannot be reached here. Lastly, it is to be kept in mind, that the GDPR mandates principles of processing that might be incompatible with AI.

3. Conclusion

I looked at the definition of AI together with the GDPR. It becomes clear that AI is a technology that is to make predictions about a certain topic derived from data that it learned from. AI is characterized through a learning process from data, a high dependency on data and a certain amount of unpredictability.

The GDPR in its technological neutrality is applicable to AI, even though certain norms in the GDPR seem to conflict with the technology. I argued before that the technological neutrality might come with legal uncertainty and potentially could rather negatively impact the protection of data subjects.

Additionally, the text of the GDPR gives rise to questions regarding the aims of protection. It is questionable whether the GDPR draws the wished or hoped for balance between the protection of data subjects and the use of personal data by companies. Also, the lobbying of mega corporations could have influenced this balance.

Lastly, it was mentioned that the principles of processing laid down in the GDPR seem to be in conflict with in the current shape and shall therefore be discussed again in the latter.

To understand better if the GDPR does govern the use of personal data for processing appropriately however, I will now examine the concept of Surveillance Capitalism.

III. Surveillance Capitalism

Surveillance has been a topic of discussion for a long time. While traditionally, the focus of defending oneself from surveillance was mostly seen in relation to a state,[63] this field changed with the development of networks of surveillance by companies.[64] Timan, Galic, and Koops propose that while surveillance nowadays in commonly defined as the carefully watching of a person or the close observation of a suspicious person, surveillance technologies do not fit these descriptions any longer. Surveillance technologies, they argue, are not especially applied to a defined realm of suspected persons but indiscriminately to all persons and omnipresent.[65] David Lyon proposes that surveillance can be defined as the "focused systematic and routine attention to personal details for purposes of influence, management, and protection of direction".[66] Another proposed definition denoted surveillance as "the collection and analysis of information about populations in order to govern their activities".[67]

It is apparent that the focus of the definition shifted from "carefully watching" somebody to collecting information about this person and using it for the purpose of analysis about him or her or influencing someone to an omnipresent watching of everybody. While current surveillance theories take more granular approaches to surveillance, I will in the following use the concept of Surveillance Capitalism as a holistic theory to assess the efficiency of the GDPR. While according to Timan, Galic and Koops this theory might be rather outdated, it is based on surveillance being widespread and everspreading, seen to be invisible or opaque, it names corporations as the

---

[63] Shoshana Zuboff, *The Age of Surveillance Capitalism- the Fight for a human future at the new Frontier of Power* (Profile Books, 2019) 53
[64] Wolfie Christl, "Corporate Surveillance in Everyday life, How Companies Collect, Combine, Analyzed, Trades and Use personal Data on Billions" (Cracked Labs, June 2017) 1, 4
[65] Tjerk Timan, Masa Galic, Bert-Jaap Koops, "Surveillance Theory and its implications for law" in Roger Brownsword, Eloise Scotford, Karen Yeung (eds), *The Oxford Handbook of Law, regulation, and technology* (Oxford University Press 2017) 732
[66] ibid.
[67] ibid.

main actors conducting surveillance and the object of surveillance as the consumer.[68] In my opinion, for the purpose of assessing the GDPR this is a solid ground assumption that will nevertheless be evaluated in the following.

Surveillance Capitalism, as the basic logic being applied in the following, was introduced by Shoshana Zuboff. She claims that capitalism has reached a mutation in which capitalism is redefined due to a change in commodities and therefore claims far more than a theory for surveillance, but a new mode of capitalism. The central commodity that is dealt with here, is behavioural data that is derived from data subjects' behaviour online and offline and transformed into predictions about future behaviour of data subjects and traded. Importantly, Zuboff mentiones AI, or in her words "machine intelligence", as part of the process of generating predictios about data subjects. [69]

According to Zuboff, this new logic of accumulation emerged from Google.[70] After implementing the Google search engine and realizing that there needs to be a revenue stream, Google discovered the potential of using data of the users that was already collected beforehand but regarded as "waste material" or "data exhaust" to make profit.[71] The company started collecting more data and feeding this data into an AI tool to predict customers' behaviours.[72] Remarkably, the data is not only used to predict future behaviour, but also to change it. [73] The predictions can also be used for personalisation, as personalisation relies heavily on knowing as much as possible about a person and therefore on mass surveillance.[74]

---

[68] Tjerk Timan, Masa Galic, Bert-Jaap Koops, "Surveillance Theory and its implications for law" in Roger Brownsword, Eloise Scotford, Karen Yeung (eds) *The Oxford Handbook of Law, regulation, and technology* (Oxford University Press 2017) 737
[69] Shoshana Zuboff, *The Age of Surveillance Capitalism- the Fight for a human future at the new Frontier of Power* (Profile Books, 2019) 8
[70] Ibid 9.
[71] Ibid 68.
[72] ibid 68-69.
[73] Karen Yeung, "Five Fears about mass predictive personalization in an age of surveillance capitalism" (2018) 8 International Data Privacy 258, 262
[74] ibid 261.

Importantly, Surveillance Capitalism comes with its own mechanisms and is not only based on a change of commodities, but also has other regularities. One of them, according to Zuboff, is surely the attempt to disguise the work practices from data subjects to circumvent opposition.[75] In fact, she proposes that the strategy of Google in Surveillance Capitalism is as follows. Firstly, Google demonstrates unique capabilities as a resource of competitive advantage, the blurring of privacy and public interests through lobbying, interchanging personell (here from the Obama administration) to Google, and lastly influencing the field of academics and public opinion.[76] Apart from this, Zuboff proposes laws of motion, or in other words new regularities for Surveillance Capitalism.

In the same line, contemporary works allege that tech-giants at the moment have developed their own ways to gain some sort of power over legislators, civil societies and the acceptance of their actions within these societies.[77] When it comes to access to legislators, influence will oftentimes be traced back to heavy investing and therefore money as a source power.[78] It is to mention that the new business trade of surveillance of data subjects that Google brought to life is highly profitable. Facebook made 97.9% of its revenue in 2020 from advertisements. This equates close to USD 85 bn in 2020.[79] To compare this number: Bulgaria's GDP in 2019 was in total roughly USD 68,6 bn.[80] This displays, which potential influence these companies can have when lobbying for their cause as well as when investing into influence on a societal level. Google's advertisement revenue in 2020 was roughly

---

[75] Shoshana Zuboff, *The Age of Surveillance Capitalism- the Fight for a human future at the new Frontier of Power* (Profile Books, 2019) 11
[76] ibid 122.
[77] Paul Niemitz, "Constitutional democracy and technology in the age of Artificial Intelligence" [2018] Phil.Trans.R. Soc. 1, 3
[78] ibid.
[79] H. Tankovska, "Facebook: advertising revenue worldwide [2021], <https://www.statista.com/statistics/271258/facebooks-advertising-revenue-worldwide/>, last accessed 12 February 2021
[80] The World Bank, "Bulgaria", <https://data.worldbank.org/country/BG>, last accessed 12 February 2021

USD147 bn.[81] Such highly profitable business will most likely not be abandoned by economic actors, but rather be intensified and defended.

When it comes specifically to lobbying in the EU, literature has long described the EU lobbying system as "elite pluralism" in which business interests are in a systematic advantage compared to the over citizen groups and non-governmental organisations.[82] Interestingly, when it came to negotiating the GDPR it was found in 2012 that members of the European Parliament were directly copy-pasting industry policy requests into legislative amendments of the proposed GDPR.[83] The attempts of having influence came from powerful private-sector firms aiming at weakening the regulation and bending it to their interests.[84] Despite the fact that proposals for changes in the text of the GDPR were brought forward through a variety of channels, most of them could be traced back to the "Silicon Valley giants".[85]

Apart from direct lobbying from the side of tech giants, the UK, in preparing for the GDPR also lobbied against rights in the GDPR such as the right to be forgotten. The UK eventually alleged that the right to be forgotten would have negative impacts on the freedom of media and could foster terrorism.[86] Interestingly, this was traced back partly to the fact that the US National Security Agency and the UK General Communications Headquarters were able to directly gather customer data from US service providers like Apple, Facebook, Google, Microsoft, and Yahoo.[87] This reflects the relevance and

---

[81] Statista, "Advertising Revenue of Google from 2001 to 2020", <https://www.statista.com/statistics/266249/advertising-revenue-of-google/>, last accessed 12 February 2021
[82] Ece Özlem Atikan, Adam William Calmers, "Choosing lobbying sides: the General Data Protection Regulation of the European Union" (2019) 39 Journal of Public Policy 543, 543
[83] ibid 545.
[84] ibid.
[85] Nihit Goyal, Michael Howlett, Araz Taeihagh, "Why and how does the regulation of emerging technologies occur? Explaining the adoption of the EU General Data Protection Regulation using the multiple streams framework" [2021] Regulation & Governance 9
[86] ibid 8.
[87] ibid.

connection of interests in Surveillance Capitalism. The lines between interests of private and public parties become blurred.

From a democratic point of view, these companies can also influence the political debate in another way. It was found, that if people know that they are being tracked, they change their behaviour.[88] Indeed, the constant surveillance one is subjected to minimizes the space of data subjects to behave slightly off social norms in privacy without facing depreciation by others.[89] This limitation of privacy can result in a subjective perception of a limitation of the freedom of speech. In fact, knowing that every action in an online environment will be tracked can easily lead to the fear of repercussions and negative consequences for the data subject if he or she gives their opinion and participates in open discourse. This can lead to a dying political discourse that is vital to a functioning democracy.

One example was given by the Wall Street Journal that reported in 2017 that Google had actively sorted out and provided funding to university professors for conducting research favouring Google's interests and policy papers in the field of law, regulation, competition and other topics. [90] This development must be taken with a lot of caution as undue influence into the democratic and societal environment together with the main control over the development of AI and other technologies in fact can be detrimental to individuals. Therefore, in the following analysis of some of the "symptoms" of company surveillance, personalized advertisement, and personalized newsfeed, will not only include the legal remedies available, but also look into possible outcomes for individuals, societies and democracy.

---

[88] Arvind Narayanan, Dillon Reisman, "The Princeton Web Transparency and Accountability Project" [2017] <https://www.cs.princeton.edu/~arvindn/publications/webtap-chapter.pdf>, last accessed 22 December 2020, 4

[89] Sheri B. Pan, "Get to know me: protecting Privacy and autonomy under big data´s penetrating gaze" (2016) 30 Harvard Journal of Law and Technology 240, 255

[90] Shoshana Zuboff, *The Age of Surveillance Capitalism- the Fight for a human future at the new Frontier of Power* (Profile Books, 2019) 126

For the individual, constant surveillance is also connected to exclusion. In fact, one can argue that this constant surveillance and the connected use of data comes with the scoring of individuals as to how much revenue they can create for the advertiser. This has the potential of creating a whole class of "low-value" individuals,[91] that can be systematically excluded from opportunities, services, and products.

It was shown in a study, that male individuals are six times more often displayed high-paying job ads than their female counterparts. It is to mention however, that this outcome is based on the historical fact, that women are less likely to be employed in high-paying jobs. During algorithmic assessment, this was interpreted as a lack of interest in high paying jobs by women,[92] while it was simply revealing longstanding discrimination of women. This exclusion however does not have to be an outcome of discrimination that had existed already, but it can be willingly caused by the advertiser. An example for that is personalized pricing. Advertisers can use personalized pricing also according to predictions about how valuable an individual can be in the future or according to a prediction on how much an individual might be willing to pay at the moment.[93] One can imagine, that these practices will undeniably lead to the exclusion from favourable offers if it is found that the individual does not have the potential of creating a certain revenue for the advertiser.

Another consequence is the general influence on human behaviour. Indeed, companies put a lot of focus on understanding how to manipulate human-technology interactions to increase the use of their services.[94]

These companies also have an impact on journalism. Traditional journalism has an important role in democracy. Investigative journalism can help

---

[91] Karen Yeung, "Five Fears about mass predictive personalization in an age of surveillance capitalism" (2018) 8 International Data Privacy 258, 265
[92] ibid.
[93] Wolfie Christl, "Corporate Surveillance in Everyday life, How Companies Collect, Combine, Analyzed, Trades and Use personal Data on Billions" (Cracked Labs, June 2017) 1, 76
[94] Brett Aho, Roberta Duffield, "Beyond surveillance capitalism: Privacy, regulation and big data in europe and China" (2020) 49 Economy and Society 187, 190

ensuring the effectiveness of governments, reducing corruption and increasing the responsiveness of elected officials.[95] In the course of the transformation into digital consumption of news, Google and Facebook quickly came to dominant market positions in the field of online advertisement and thereby deprived journalistic newspapers and online magazines from their revenue streams.[96] This is one of the reasons for a dying press.

With this change also comes the fact, that companies like Google and Facebook that are now became the main source of political information, especially to younger people.[97] Especially when it comes to elections, this can lead to distortions of election results. In the light of experiments on Facebook users, this is highly problematic. A study conducted in November 2010 (at the day of the US congressional elections) focused on the question, whether political behaviour can spread through online networks (here Facebook).[98] Within the experiment, users of at least 18 years of age were sorted into three different groups. The first group was a "social message" goup in which users were animated through their newsfeed to vote and provided a clickable button reading "I voted" together with an indication how many other Facebook users had already voted and pictures of the user´s friends that had already voted.[99] The second group, the "informational message" group, was shown the same content in general, but was not displayed the profile pictures of friends that already had voted. The third group was the control group that did not receive any message on their newsfeed.[100] It was found that the social message on

---

[95] Rasmus Kleis Nielsen, Richard Fletcher, "Democratic Creative Destruction? The Effect of a changing Main Landscape on Democracy", in Nathaniel Persily, Joshua A. Tucker (eds) *Social Media and Democracy- The state of the field, Prospects for Reform* (Cambridge University Press, 2020) 141
[96] ibid 144.
[97] Paul Niemitz, "Constitutional democracy and technology in the age of Artificial Intelligence" [2018] Phil.Trans.R. Soc. 1, 3
[98] Robert M. Bond, Christopher J. Fariss, Jason J. Jones, Adam D. I. Kramer, Cameron Marlow, Jaime E. Settle, James H. Fowler, "A 61-million-person experiment in social influence and political mobilization" (2012) 489 Nature 295, 295
[99] ibid.
[100] ibid.

Facebook increased the election turnout in total by 340 000 votes.[101] It was also shown that social mobilization is significantly more effective than informational mobilization alone.[102] While here the influence might have been positive, the influence that Facebook can potentially have on elections has to be taken with caution. Especially in the light of negative examples like Cambridge Analytica.[103]

To sum up shortly, Surveillance Capitalism is the theory that will be used in the following and that is thought of to be a mutation of capitalism shifting to the indiscriminated and omnipresent collection of data. It was shown previously, that companies, most and foremost techcompanies are thought of as Surveillance capitalists that are not only responsible for big parts of the surveillance on their customers, but are also seeking to influence their environment to ensure their positions. Importantly, while Surveillance Capitalism is not a technology, it is highly related to it. The development of AI facilitates mass collection and analysis of data and is therefore an important topic when it comes to mass surveillance.

I will now go on and examine the use of AI in personalisation and potential pitfalls for rules laid down in the GDPR in Surveillance Capitalism.

1. Personalized advertisement

Personalized advertisement means advertisement that is only shown to a certain group of people according to their attributes.[104] The field of advertisement includes several actors. Advertisers, that decide which users

---

[101] Robert M. Bond, Christopher J. Fariss, Jason J. Jones, Adam D. I. Kramer, Cameron Marlow, Jaime E. Settle, James H. Fowler, "A 61-million-person experiment in social influence and political mobilization" (2012) 489 Nature 295, 297
[102] ibid, 297
[103] Carole Cadwalladr, Emma Graham-Harrison, "Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach", <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>, last accessed 5 May 2021
[104] Till Speicher, Muhammad Ali, Giridhari Venkatadri, Filipe Ribeiro, George Arvanitakis, et al., "Potential for Discrimination in Online Targeted Advertising" [2018] <https://hal.archives-ouvertes.fr/hal-01955343> last accessed 22 December 2020, 1, 2

will see the advertisement, ad platforms such as Google, that aggregate data about their users, and make it available for targeting purposes, and the users of ad platforms that at the same time are subject to targeted advertisement.[105] The personalisation or targeting of advertisement can either be based on a selection of attributes from the advertiser, the specification of data subjects the advertiser wants to target (by means of email addresses for example) or by targeting data subjects that are similar to the set of customers the advertiser already has.[106]

Personalized advertisement is said to have benefits for advertisers and data subjects. The use of AI in the field of advertisement enables companies to target possible customers that could be directly interested in their products. This decreases the cost of advertisement and at the same time is convenient for the data subject. In fact, it was found that companies were able to increase their sales over 10% by using personalised advertisement.[107] Personalized services can also reduce information overload or act as a decision aid because the cognitive efforts to make a decision are reduced.[108]

It is to mention however, that there are many ways in which discrimination can be furthered through personalisation. One example of this would be the requirement of targeting data subjects with a job ad, which exclude people over 40 and females. Another possibility is the combination of data provided for example by Facebook and public sources and therefore derive special categories of data and target groups according to ethnicity.[109] While this is

---

[105] Till Speicher, Muhammad Ali, Giridhari Venkatadri, Filipe Ribeiro, George Arvanitakis, et al., "Potential for Discrimination in Online Targeted Advertising" [2018] <https://hal.archives-ouvertes.fr/hal-01955343> last accessed 22 December 2020, 1, 2
[106] ibid 3.
[107] Blake Morgan, "The 7 Best Examples Of Artificial Intelligence To Improve Personalization"[2019], <https://www.forbes.com/sites/blakemorgan/2019/01/24/the-7-best-examples-of-artificial-intelligence-to-improve-personalization/?sh=309545a3c4ed>, last accessed 9 November 2020
[108] Sabrina Karwatzki, Olge Dytynko, Manuel trend, Daniel Veit, "Beyond the Personalization-Privacy Paradox: Privacy valuation, Transparency Features, and Service Personalization" (2017) 34 Journal of Management Information Systems 369, 371
[109] Till Speicher, Muhammad Ali, Giridhari Venkatadri, Filipe Ribeiro, George Arvanitakis, et al., "Potential for Discrimination in Online Targeted Advertising" [2018] <https://hal.archives-ouvertes.fr/hal-01955343> last accessed 22 December 2020, 7

not a problem per se, it can lead to exclusion. One can imagine that job ads could be displayed only to certain ethnic groups and therefore exclude other ethnicities from career opportunities.

Importantly, as the aim is to get the users' attention, companies will not only track the consumers' online behaviour and try to learn from it, but also try to manipulate the user into coming back.[110] This can be completely harmless and has the benefit that through the tracking and monitoring activities online, the consumer does not have to conduct a lengthy search for things they are interested in, but will most likely be shown information that is interesting for them, based on already targeted showing of news and advertisement. This gives the consumer an enhanced level of convenience and will typically take place on social media platforms and YouTube.[111]

As nothing is without flaws, there is a possibility that the personalisation is inaccurate or otherwise faulty. This could lead to over-personalisation, meaning that data subjects could be encouraged to act on their impulsive present selves.[112] In these cases, the personalisation feeds into the short term wishes of individuals and manipulates them into preferring to satisfy these rather than long-term wishes that could be beneficial for the data subjects. While this is the general workings of advertisement, the use and analysis of personal data will lead to a much better picture over the wishes of individuals and therefore have the potential to be more effective. While efficiency is not a problem per se, it becomes a problem when the data subject is subconsciously tricked into a buying behaviour that does not benefit the data subject. The data subject needs to be aware of these practices to shield him or herself against these privacy invasive advertising practices to not be fooled.

---

[110] Kris Shaffer, *Data versus Democracy, How Big Data Algorithms Shape Opinions and Alter the Course of History*,(apress, 2019) 12

[111] Lucy Maguire, "Gen Z is reinventing social media marketing" <https://www.voguebusiness.com/consumers/gen-z-reinventing-social-media-marketing-tiktok-youtube-instagram-louis-vuitton>, last accessed 12 February 2021

[112] A. Sheri, B. Pan, "Get to know me: protecting Privacy and autonomy under big data´s penetrating gaze" (2016) 30 Harvard Journal of Law and Technology 240, 251

Personalisation can also be inaccurate. This can lead to violations of personal autonomy. An example raised here is the LinkedIn proposals of jobs that are marked with "Jobs you may be interested in". In cases where these recommendations are significantly under the qualification of the data subject, the data subject might be manipulated into applying for jobs that it is overqualified for or into working for less salary than appropriate for qualification and experience.[113]

The previous example illustrates the impacts advertisement can have on data subjects. Even though efficient advertisement seems to make sense in the first place, efficiency should not be an argument when it leads to the manipulation of data subjects and their subsequent change of behaviour or their self-perception to their detriment.

Under certain circumstances however, it can also limit the data subject´s suggested preferences and give limited choices, for example, when it comes to book, music, or newsfeed. Additionally, it can lead to denial of certain services and goods and unjustified discrimination.[114] This leads to questions of fairness in distribution of goods and rights.

The basis of personalized advertisement, as stated beforehand, is the collection of a vast amount of personal data. To collect this data, the legal ground of consent is a frequent basis. Therefore, I will examine consent in the following and lay particular focus on the question whether the logic underlying consent is compatible with Surveillance Capitalism.

1.1. Consent

The requirement of consent is laid down in Article 6 (1)(a) GDPR and mandates consent as a basis for lawful processing of personal data. As consent has been subject of longstanding discussion, I will first examine the ideological basis of consent and raise the question whether this is compatible

---

[113] A. Sheri, B. Pan, "Get to know me: protecting Privacy and autonomy under big data´s penetrating gaze" (2016) 30 Harvard Journal of Law and Technology 240, 251

[114] Article 29 Working Party, "Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679", (WP251 rev. 01, 3 October 2017), 6

with the laws of motion of Surveillance Capitalism and then go to examine the legal requirements for consent.

1.1.1. Ideological basis of consent

Consent has been subject to much criticism and discussion under the GDPR. Therefore, I propose that it makes sense to first examine what the ideological basis of consent can tell about the function under the GDPR.

The GDPR aims to enable the data subject to make use of information control. Consequently, consent is to be seen as tool for exercising this control. The GDPR mentions that consent must be freely given, or in other words underlying for the exercise of control is a certain amount of freedom and choice as well as oversight.

When turning to the question of freedom, Amartya Sen proposes that freedom is important for two reasons- it gives the opportunity to pursue one's objectives and attaches importance to the process of choice itself. Freedom therefore has an aspect of opportunity and process.[115] To be able to make a decision freely, the data subject is not to be restrained in his or her capability of making this decision, meaning that nobody is to give the answer for the data subject. In this way, one can regard the idea of information control as a measure to further the data subject's freedoms and privacy.

It seems however, that this control is rather an illusion. Shoshana Zuboff describes it as follows: "Surveillance capitalists know everything about us, whereas their operations are designed to be unknowable to us."[116] This reveals that it might be a structural change that is necessary when thinking of data protection laws. Critically, from an individual point of view however, this abundance of control over one's data and lack of information is oftentimes met by paralysing coping mechanisms like cynicism or ignorance out of frustration and helplessness.[117]

---

[115] Amartya Sen, *The Idea of Justice,* (Penguin Books, 2010) 229
[116] Shoshana Zuboff, *The Age of Surveillance Capitalism- the Fight for a human future at the new Frontier of Power* (Profile Books, 2019) 11
[117] ibid.

While it is clear, that the measure of consent and the underlying rationale of data protection laws is focused on control over personal data by the data subject, the rationale of Surveillance Capitalism is based on the invisibility of data collection and the obscuring of profiling. This sets a very high burden on the measure of consent. In other words, the underlying logic of the use of consent is in clear contrast to the rationale of Surveillance Capitalism. This indicates, that consent will suffer from tensions between the two ideological bases. To understand however, whether the GDPR is prepared for Surveillance Capitalism, I will now examine the requirements for consent under the GDPR.

1.1.2. Requirements of consent under the GDPR

Consent under data protection law is defined as "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".[118]

Consent is free when the data subject is given a real choice and actual control over his or her data. This includes also that the data subject needs to have a right to withdraw consent easily.[119]

Another requirement is that in cases where a service may involve multiple processing operations for more than one purpose, the data subject shall have the right to consent or not to each purpose independently.[120] This shall lead to more transparency and maybe enhance data subjects' understanding for the amount of data that is collected and the manifold processing purposes the

---

[118] Article 4 (11) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1

[119] Article 7 (3) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1

[120] Recital 43 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1

controller wants to conduct. While this measure is to enhance the transparency of processing, it can be questioned whether transparency is reached when the data subject is confronted with many different purposes he or she must assess separately. This should be dependent on the amount of different purposes, however.

Additionally, the information that is given to the data subject needs to be easily distinguishable from other information if the consent is given in the context of a written declaration that also concerns other matters.[121] The controller can therefore not hide the information on planned processing activities between other information that is not related to the request for consent.

When it comes to the requirement of the consent to be informed, the data subject does not only need to have necessary information to understand the processing operations, but also needs additional information about the controller. According to the European Data Protection Board, the data subject needs to be informed at least about the controllers identity, the purpose of each of the processing operations for which the consent is sought, the type of data that will be collected and used, and the right to withdraw consent. The data subject should also receive information regarding whether the data is used for automated decision-making and possible risks of data transfers due to the absence of an adequacy decision and appropriate safeguards.[122] Interestingly, inferences are not mentioned separately even though the inferences to be drawn can have significant effects on data subjects. Inferences could for example reveal something that the data subject did not want to disclose such as moods, feelings, or simple secrets a person wants to keep.

---

[121] Article 7 (2) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1

[122] European Data Protection Board, "Guidelines 05/2020 on consent under Regulation 2016/679"(edpb, 4 May 2020), 15-16

Inferences could also include sensitive information, like data on one's mental state or health. The simple process of drawing inferences can therefore reveal things about a person, the person might not have expected and therefore the person might not have made an informed choice. This however, is against the idea of consent and would therefore render consent invalid.

It is questionable, whether the data subject will understand which information will be used and which inferences can and will be generated in the context of personalisation. This is due to the amount of data that can be used and the seemingly missing connection to the advertisement when excessive collection takes place.

As the used technologies for profiling are constantly increasing in complexity, the disclosures and privacy notes will oftentimes be difficult to read and understand.[123] This is clearly against the definition of consent as given in article 4 (11) GDPR that states that the data subject is to give an informed and clear indication of his or her will.

Even were the data privacy policy and disclosure documents to fulfil these requirements, this does not necessarily lead to a sound understanding from the data subject. It was shown, that giving more information to the data subject might not always be the best choice. In fact it was proven that the more information is given to the data subject, the less data subjects are able to make rational decisions in line with their values of privacy based on this information.[124] Additionally, the frequency with which data subjects are confronted with decisions about their privacy is extremely high and it can therefore have blunting effects that lead to the data subject being overwhelmed with the information given and abstaining from rational decisions about his or her privacy. It is at hand, that effective actions against

[123] I. Van Oijen, Helena U. Vrabec, "Does the GDPR enhance consumers´control over personal data? An analysis from a behavioural perspective" [2019] Journal of Consumer Policy 91, 95
[124] ibid.

the loss of privacy can only happen based on the understanding of the data subject. With this missing, actions against the processing will be difficult.

The consent needs to be given through a clear and affirmative act. This means, the data subject is to give his or her consent through an active motion or declaration. The use of pre-ticked opt-in boxes in the online environment does not fulfil this requirement. The same is true for cases in which the data subject stays inactive or silent. Therefore, the mere proceeding with a service cannot be treated as consent where the data subject does not react to the request for consent.[125] Acknowledging this is important, because websites still use default options to opt-in to a service that has been proven to in fact not lead to a conscious decision from the data subject.

Additionally, a special weight is given to possible power imbalance arising that could hinder the data subject from exercising their free will and rather leads them to accept based on the fear or actual risk of detrimental effects.[126] Recital 43 proposes that it is unlikely that public authorities could ask data subjects for consent because of the obvious power imbalance. The same is true for requests for consent in employment contexts according to the European Data Protection Board.[127] Noteworthy, account shall not only be taken of actual detrimental effects, but also the fear of detriment for the data subject.[128]

The European Data Protection Board also states that this power imbalance cannot only occur in employment and public authority contexts, but there can also be other relationships that have to be treated similarly. Recital 43 GDPR states in that connection that to assess whether there is an imbalance in the relationship between the controller and the data subject all circumstances of

[125] European Data Protection Board, "Guidelines 05/2020 on consent under Regulation 2016/679"(edpb, 4 May 2020) 18
[126] European Data Protection Board, "Guidelines 05/2020 on consent under Regulation 2016/679"(edpb, 4 May 2020) 9
[127] ibid.
[128] European Data Protection Board, "Guidelines 05/2020 on consent under Regulation 2016/679"(edpb, 4 May 2020) 9; Article 29 Working Party, "Opinion 15/2011 on the definition of consent" (WP187, 13 July 2011) 13

the specific situation have to be taken into account.[129] It also states, that it is presumed that the consent was not freely given if the data subject is not allowed to separately consent to different processing operations even though it would be appropriate in the individual case.[130] Additionally, consent is not presumed to be freely given if the data subject has no genuine or free choice.[131]

When thinking of consent in an online environment, there are companies that could fulfil this threshold. When taking Facebook as an example, the company holds several very popular services like the Facebook app, Instagram, and WhatsApp. In fact, Facebook has acquired more than 90 companies.[132] I propose here, that through the fact that the company is the dominant figure in social networking and social media platforms, there is no real alternative for the data subject to using Facebook and its related services. The Article 29 Working Party supported the possibility in its opinion on the definition of consent. It states that when registering with a social network service, the data subject is oftentimes required to consent to receiving behavioural advertisement and left with no alternative. It then refers to the importance that some social networks have acquired for some categories of users and propose that data subjects will therefore rather accept the behavioural advertisement than being partially excluded from social interaction.[133] Even though there is no legal pressure that can necessarily be

[129] Recital 43 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1
[130] ibid
[131] Recital 42 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1
[132] Mark Glick, Catherine Ruetschlin, "Big Tech Acquisitions and the Potential Competition Doctrine: The Case of Facebook" (2019), Institute for New Economic Thinking, < https://www.ineteconomics.org/uploads/papers/WP-104-Glick-and-Reut-Oct-10.pdf>, last accessed 1 February 2021
[133] Article 29 Working Party, "Opinion 15/2011 on the definition of consent" (WP187, 13 July 2011) 13

assumed here, I argue that social exclusion from services should count as the fear of detriment that suffices to render the option for consent void.

To estimate which companies should be able to use consent for their data collection, I propose that a standard could be established that considers whether the controller in question has a dominant position on the market, the amount of users of this service, the transparency of the processing taking place, the amount of processing purposes and data that is collected, and whether there is alternatives to the controller that have a similar quality. I propose that the size of the controller together with the amount of users of the service is important as it does give an indication not only on a sheer imbalance of knowledge, but it also indicates potential social pressure for using a service. The criteria of processing purposes and amount of data collected is proposed because the more data and processing purposes are taking place, the less it can be expected that the data subject would understand and expect the processing taking place.

In the case of Facebook for example, it is to say that Facebook belongs to the largest platforms when it comes to the collection and use of personal data from data subjects for advertisement purposes.[134] Additionally, Facebook also collects information about data subjects through other Facebook products or related services such as Instagram, Messenger, and Whatsapp.[135] Additionally, it was recently found that the scope of consent that is asked for from Facebook is difficult to understand for the data subject.[136] Another topic of concern are inferences that are derived from the personal data Facebook is collecting from the data subject. It seems, that inferred sensitive data, that falls under the category of special categories of data under the GDPR and enjoys special protection, is not sufficiently protected.[137] When it comes to inferences in general, it is not clear which information might be inferred and

[134] Sourya Joyee De, Abdessamad Imine, "Consent for targeted advertising: The case of Facebook" (2020) 35 AI & Society 1055, 1056
[135] Sourya Joyee De, Abdessamad Imine, "Consent for targeted advertising: The case of Facebook" (2020) 35 AI & Society 1055, 1059
[136] ibid.
[137] ibid.

which third parties are involved.[138] Lastly, the default settings for consenting are to accept intrusive privacy settings.[139] Overall, it is questionable whether consent as used by Facebook does comply with the GDPR. Due to the imbalance not only in power but also in knowledge and the opaque nature of the use of personal data by Facebook, I propose that consent as enshrined in the GDPR and with the aim of enabling the data subject to make a conscious and free choice, is unlikely to be reached.

While I acknowledge, that one could allege paternalism here, abandoning consent in cases where a power imbalance is indicated does not mean that the data subject cannot use a service. Rather, it puts the responsibility on the controller to find another ground for processing and justify processing thereby. It is to mention however, that the abandoning of consent in these cases can only have beneficial impacts in the long run if there is a strict control over the legal grounds sought as a basis for processing.

To sum up shortly, I would like to emphasize, that consent as a measure of control over one's personal data is dependent on the understanding and possibility of the data subject to evaluate his or her options regarding his or her privacy. Consent should be a freely given, specific, informed decision that is communicated in a clear and affirmative way. Power imbalances and lack of understanding however, can impact consent and should therefore be taken seriously. I propose that social media platforms like Facebook might be in a relationship with the data subject that is characterized by a power imbalance between the data subject and the controller that have the potential to render consent invalid.

1.1.3. Conclusion

When examining the ideological base of consent and the GDPR in general, it becomes clear that the GDPR aims at enabling the data subject to make decisions in his or her interest through consenting or refusing to consent.

---

[138] Sourya Joyee De, Abdessamad Imine, "Consent for targeted advertising: The case of Facebook" (2020) 35 AI & Society 1055, 1060
[139] ibid, 1061.

However, it was shown that this freedom is impacted by the fact that while the GDPR aims at transparency, the logic of surveillance capitalism aims at being intransparent. This can be seen in several instances when looking into the use of consent and leads to its ineffectiveness in cases where the data subject is overwhelmed with information that is not understandable to the data subject or where he or she fears of detriment.

1.2.Profiling

The personalisation of advertisement will oftentimes be based on profiling. Profiling according to the GDPR 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 analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements".[140] The definition makes clear, that it is about drawing assumptions about the individual, not necessarily truths.

In general, profiling follows three technical stages. First, data, for example the content of a shopping basket, a telecommunications bill, a list of trips on public transport, is collected.[141] Second, the data collected is analysed by means of data mining in order to detect patterns and to create profiles. Third, the profiles are used for deducing knowledge of the behaviour of persons.[142]

While one could argue that the categorizing of data subjects according to characteristics can be done by a human, the considerable amount of data that can be processed, together with the overall efficiency that the use of AI is able to deliver oftentimes exceed human abilities.[143] Profiling activities will use a

---

[140] Article 4 (4) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1

[141] Elena Gil González, Paul de Hert, "Understanding the legal provision that allow processing and profiling of personal data- ana analysis of GDPR provisions and principles" [2019] (ERA Forum), 598, 609

[142] ibid 609.

[143] Leah Fainchtain, "AI Algorithms Are Changing Personalization: Here's How" (2020), < https://developer.ibm.com/recipes/tutorials/ai-algorithms-are-changing-personalization-heres-how/>, last accessed 5 February 2021

certain amount of automation.[144] The downside, however, is that within the process of machine learning biases can occur not only in data sets that could stem from previous discrimination against a certain group of people, but biases can also be generated through machine learning. [145] These biases can occur through learning from examples and the algorithm determining by itself what it deems relevant.[146]

The data collection by companies will oftentimes be invisible and take place without knowledge or consent of the data subject.[147] When it comes to web applications, tracking is conducted by the website provider or third parties. Cookies are widely used by first and third parties for tracking on websites. Recently, websites and trackers increasingly turn to techniques like browser fingerprinting, that stands out as a technique because it is more difficult for the data subject to protect him- or herself from tracking and oftentimes does not leave any traces on the consumers device.[148] Importantly, these fingerprints can be used to uniquely identify consumers devices without cookies.[149]

This is problematic when it comes to the enforcement of rights and, most and foremost, the detection of treatment that would allow for action. The data subject needs to know of the existence of profiling to be able to assess the profiling that takes place and to act in the case of unjustified discrimination. In fact, the GDPR does mandate information rights for the data subject in

---

[144] Elena Gil González, Paul de Hert, "Understanding the legal provision that allow processing and profiling of personal data- ana analysis of GDPR provisions and principles" [2019] (ERA Forum), 598, 608
[145] Laurens Naudts, "How Machine Learning Generates unfair inequalities and how data protection instruments may help in Mitigating Them" in Ronald Leenes, Rosamunde van Brakel, Serge Gutwirth, Paul de Hert (eds) "Data Protection and Privacy, the Internet of Bodies "(Oxford: Hart Publishing 2018) 76
[146] ibid.
[147] Wolfie Christl, "Corporate Surveillance in Everyday life, How Companies Collect, Combine, Analyzed, Trades and Use personal Data on Billions" (Cracked Labs, June 2017) 1, 5
[148] Arvind Narayanan, Dillon Reisman, "The Princeton Web Transparency and Accountability Project" [2017] <https://www.cs.princeton.edu/~arvindn/publications/webtap-chapter.pdf>, last accessed 22 December 2020, 5
[149] ibid.

articles 13 and 14 for cases where data was directly provided by the data subject and in cases where the data was not obtained directly from the data subject. This information also includes the identity of the controller as well as information on the data collected and the rights the data subject would have in reaction to the processing. Therefore, the practice of not informing the data subject about processing of personal data does violate the GDPR.

Within profiling, one can differ between individual profiling and group profiling.[150] Individual profiling means that the information about the individual is collected and analysed to predict future behaviour and understand the person better. Individual profiling raises severe problems as it allows for individually targeted advertisement or news provision that can take advantage of individual vulnerabilities. An example is the possibility of analysis of click-through behaviour of the data subject to identify when the data subject is feeling low and is therefore more vulnerable to make impulsive purchases.[151]

Group profiling on the other side can either take place in relation to already existing groups or it can sort people into certain groups. Examples mentioned in literature are women who have visited an abortion clinic as an example for people who share characteristics. The women will not know who is part of the group (of women who went to an abortion clinic) but will be sorted into this group because they share a characteristic.[152] An example for people being sorted into a group would be people that are more likely to develop a certain disease. The people will not always fulfil all risk factors, but will all be likely to develop a certain disease.[153] The risk with the latter can be that attributing certain characteristics to individuals according to the ascription to a group can

---

[150] Elena Gil González, Paul de Hert, "Understanding the legal provision that allow processing and profiling of personal data- ana analysis of GDPR provisions and principles" [2019] (ERA Forum), 598, 608

[151] Karen Yeung, "Five Fears about mass predictive personalization in an age of surveillance capitalism" (2018) 8 International Data Privacy 258, 261

[152] Privacy International, "Data Is Power: Profiling and Automated Decision-Making in GDPR" [2017] 3 <https://privacyinternational.org/sites/default/files/2018-04/Data%20Is%20Power-Profiling%20and%20Automated%20Decision-Making%20in%20GDPR.pdf>, last accessed 9 February 2021

[153] ibid.

lead to a false assignment of characteristics and lead to unfair results.[154] In other words, a person belonging to a group will be treated according to the characteristics that are ascribed to the group, not as an individual.[155] This could lead to unfairness in the sense that the effects of the processing of the personal data of the data subject might not be justifiable in the individual context. An example for this would be the denial of a loan based on the attribution to a group that is deemed to be unlikely to pay it back due to low income, without considering the special circumstances of the data subject.

Another problem that is deeply connected to profiling and the mass surveillance of individuals that comes with it, is the fact that the power imbalance between the profiler and the data subject are increased in the sense that the mere knowledge of vulnerabilities, interests and preferences, gives more power to the profiler and enhances the risk that the profiler might abuse this power.[156]

The claims that profiling as a base for personalisation for advertisement benefits the data subject by delivering relevant content to them, is also problematic in the light of the values that are given to individuals in the process. Data subjects will not only be evaluated, filtered out and scored in the process, but the profiling will also reveal how "useful" the data subject will probably be to the shop or retailer that wants to advertise his or her service. This means, that in the process of profiling, the individual will be oftentimes scored according to the buying habits, wealth and so forth. If an individual is seen to have the potential of delivering profits to the advertiser, he or she will receive generous and attractive offers, while an individual that is unlikely to deliver profits, will not receive these offers. These individuals will be excluded from the benefits and therefore in the long run be harmed in

---

[154] Elena Gil González, Paul de Hert, "Understanding the legal provision that allow processing and profiling of personal data- an analysis of GDPR provisions and principles" [2019] (ERA Forum), 598, 609

[155] Elena Gil González, Paul de Hert, "Understanding the legal provision that allow processing and profiling of personal data- an analysis of GDPR provisions and principles" [2019] (ERA Forum), 598, 609

[156] Karen Yeung, "Five Fears about mass predictive personalization in an age of surveillance capitalism" (2018) 8 International Data Privacy 258, 261

their autonomy as the concept of autonomy necessarily is based on having the choice between options. Evidently, this is most important in cases where the individual was wrongly "classified" and therefore does not benefit from offers relevant to him or her. The data subject could be deprived from the options.[157] In this context, the first hurdle for assessing the rights the GDPR might provide for the data subject will be that the data subject might not be aware of the discrimination as he or she does not receive certain offers in the first place.

Again, the focus lays on the fact that the GDPR aims at giving control over personal data to the data subject. The controll that is aimed at, is unlikely to be achieved in cases where the data subject is not aware of the profiling itself or the potential consequences for his or her privacy.

To sum up shortly, it is to say that profiling is the art of using collected data about individuals that is then used to analyse and evaluated these persons. It becomes problematic where the profiling leads to the abuse of inferred vulnerabilities, where the knowledge about the data subject is intrusive itself, and where knowledge is used as a source of power to misuse to the detriment of the data subject.

1.3.Inferences

When attempting to target advertisement to an individual or a group of individuals, it will be crucial to understand the needs, as well as preferences of an individual. For this reason, one does not only want to use the data that can be gathered directly through webpages, likes given on Facebook etc, but one will also attempt to derive knowledge from the given by deducing information, or infering knowledge, about a data subject. Inferences that are generated are the result of the use of an AI tool. The tool or analytical model uses source data that it is fed, to gain more insights of a person or detect patterns. In other words, inferences are conclusions and predictions that are

[157] Karen Yeung, "Five Fears about mass predictive personalization in an age of surveillance capitalism" (2018) 8 International Data Privacy 258, 261

derived from available data.[158] While inferences are crucial for personalisation, they can also give rise to several problems. Inferences can create significant harms for data subjects, such as over-and inaccurate personalisation, violation of due process and discrimination.[159]

Inferences made from personal data have the potential to fall into the realm of special categories of data.[160] This means, that the input data to the AI tool can be personal data, but the data that is inferred while analysing this personal data and therefore the output data of the AI tool is sensitive. As an example one could imagine the detection of certain diseases like diabetes or cancer through online searches or certain buying habits of goods. There can also be other secrets apart from health that a data subject might not want to be revealed such as sexual orientation. In general, there are two different types of inferences that can generate sensitive information: Firstly, qualitative conclusions about a data subject can be made that are reached by using quantitative data and inferences related to a person´s attribute. Secondly, attributes or demographic characteristics can be found using data on the behaviour of the data subject.[161] When special categories of data are created, explicit consent, or other legal bases as laid down in article 9 GDPR have to be sought. This can be problematic where it was not previously expected that special categories of data would be created.

Importantly, inferences drawn will oftentimes be surprising. This is due to the fact, that correlations within data sets will be found and conclusions will be drawn about the given data.[162] These inferences are not necessarily always right. This is especially problematic not only when it comes to special categories of data, but also when it comes to the expectations of the data

---

[158] Joe O'Callaghan, "Inferential Privacy and Artificial Intelligence - A New Frontier?" [2018] < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3301354>, last accessed 22 December 2020, 2
[159] A. Sheri, B. Pan, "Get to know me: protecting Privacy and autonomy under big data´s penetrating gaze" (2016) 30 Harvard Journal of Law and Technology 240, 250
[160] ibid 247.
[161] A. Sheri, B. Pan, "Get to know me: protecting Privacy and autonomy under big data´s penetrating gaze" (2016) 30 Harvard Journal of Law and Technology 240, 247
[162] ibid 249.

subject. The data subject, when consenting or refusing to consent to processing has to be aware of the possible consequences of the potential outcomes of the consent. It is questionable however, whether the data subject is aware of potential pitfalls of inferences and their consequences. Also in the light of cases where individuals are not aware which inferences are drawn the data subject cannot request the inference to be removed or corrected. This can lead to discriminatory treatment from the advertiser.

Drawing inferences can also infringe the purpose limitation that is laid down in the GDPR. This would be the case, when it could not have been reasonably expected that inferences would have been generated in this area, given the source data, or in cases where the inference is privacy invasive.[163] An example could be if the ethnicity of a person is inferred based on the area in which a person lives and his or her income.

To sum up shortly, despite their importance for personalisation, inferences can create several problems. Firstly, inferences have the potential to belong to the realm of special categories of data and therefore to touch a very private part of data subject's life. Secondly, the data subject might not always be aware and understand the potential inferences that can be drawn about him or her and therefore might not be able to consent to processing that involves drawing inferences. Thirdly, surprising outcomes when drawing inferences can also impact the compatibility with the purpose limitation laid down in the GDPR.

1.4.Data minimisation

When it comes to personalisation, be it news or advertisement, the amount of data that is collected is already problematic when considering the GDPR. As it was seen beforehand that a huge amount of data is collected and analysed, one needs to think about the data processing principles that are laid down in the GDPR, especially the principle of data minimisation. The principle of data

[163] Joe O'Callaghan, "Inferential Privacy and Artificial Intelligence - A New Frontier?" [2018] <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3301354>, last accessed 22 December 2020,13

minimisation can be found in article 5 of the GDPR and covers several traditional principles, such as the collection limitation, data quality, purpose specification and use limitation.[164] Data must be relevant and should not be outdated or wrong. Additionally, the Article 29 Working Party proposes, that the controller should be able to explain and justify the need to collect and hold data or use aggregated or anonymized or pseudonymized data for profiling.[165]

As this principle combines several ideas, it is to note that the GDPR provides specific norms for data quality in the sense that it entails the right to access, rectification, and erasure together with the necessary information obligations from the side of the controller to ensure that the data subject is aware of the information held by the controller. These rights are crucial for the data subject as the data subject is said to gain at least some control over the data held on him or her.

It was proposed to loosen the principle of data minimization to enable the greater use of big data. [166] I do not agree with this proposal as this would hamper the protection of privacy. In fact, the justification for this principle would be rendered void. The data minimization principle is based on two convictions. Firstly, where less data is gathered in the first place the data controller has less opportunities to infringe the rights of data subjects.[167] Secondly, the longer the data controller holds personal data, the bigger the risk of personal data to be hacked.[168]

---

[164] Lilian Mitrou, "Data Protection, Artificial Intelligence and Cognitive Services- Is the General Data Protection Regulation (GDPR) 'Artificial Intelligence-Proof?'" [2019] <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3386914> last accessed 10 December 2020, 1, 49

[165] Article 29 Working Party," Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679" (WP251 rev. 01, 3 October 2017), 11

[166]Tal Z. Zarsky, "Incompatible: The GDPR in the Age of Big Data" (2017) 47 Seton Hall Law Review 995, 1011

[167] Lilian Mitrou, "Data Protection, Artificial Intelligence and Cognitive Services- Is the General Data Protection Regulation (GDPR) 'Artificial Intelligence-Proof?'" [2019] <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3386914> last accessed 10 December 2020, 1, 49

[168] Tal Z. Zarsky, "Incompatible: The GDPR in the Age of Big Data" (2017) 47 Seton Hall Law Review 995, 1010

Indeed, the focus should lay on the fact that the collected data is data that refers to an individual that can be significantly harmed where wrong or outdated information is processed and used for decision making. Especially in the light of AI and machine learning it is important to note that the principle of data minimization gains indispensable value as deletion of data is likely to be infeasible so far.[169] It is to mention additionally, that the principle of data minimization sets a minimum standard that should be seen as the base for all rights of the data subject concerning access, rectification and erasure. Abandoning or further weakening this principle in favour of endless data collection and for the benefit of companies that can hold this information for eternity cannot be wished for.

I propose that the principle of data minimisation should gain more attention and data collection should be limited to what is necessary for the controller to be able to provide the services or fulfill the contract that the data subject has with the controller. While it seems unrealistic that the data minimisation principle will be strengthened as it does have potential to harm the omnipresent data collection including every single click, it could have its benefits to establish a stronger principle for data minimisation. It could potentially have the effect that AI models are designed differently and therefore influence the development of AI positively.

1.5.Storage limitation

The storage limitation is also contained in article 5 GDPR and obliges the controller to limit the storage of data to a certain amount of time. When it comes to AI this can be problematic, as AI systems learn from the data that is provided and therefore "stores" what is learned from the data. It is questionable, whether AI actually "forgets" data. This is mostly due to the data sets the AI learns from. If this is enough to infringe the storage limitation, however, will be examined in the following.

---

[169] Eduard Fosch Villaronga, Peter Kieseberg, Tiffany Li, "Humans forget, machines remember: Artificial Intelligence and the Right to Be Forgotten" (2018) 34 Computer Law and Security Review 304, 309-310

Firstly, it is to be reminded that the AI model as such learns from data. For this reason, it is necessary to look at deletion of data in relational databases as they are oftentimes used as base for machine learning and AI models. Relational databases work with indexing information and therefore referring from one database to another and connecting knowledge throughout different datasets.[170] This also means that data might be stored at various locations within the internal data mechanisms and in several backups, logfiles and different replicated databases.[171] When data is to be deleted from such a database, it oftentimes has to be overwritten with random information. This can cause inconsistencies within the database or affect its usability.[172] Additionally, when data is deleted via the interface of the database system, the data is often not overwritten, but marked as deleted and removed from search indexes.[173] It is argued that deleting and overwriting means exceptional additional effort with potential seriously negative effects on the efficiency of the AI model.[174]

Secondly, while the deletion from relational databases causes tremendous problems, the case does not lay different for AI models. The deletion of data from AI models can take place in two ways. Either, the model can be trained with an amended training set or the model itself can be amended after the training phase. While the former causes significant energy , time, and labour costs, the latter is difficult and oftentimes not feasible. It is additionally argued in literature that machine learning algorithms that have the potential of quick and easy removal of data from AI models is not developed yet.[175] Another problem to be mentioned is also that the removal of individual data will oftentimes have little impact on the learned patterns by the AI tool. This

---

[170] Eduard Fosch Villaronga, Peter Kieseberg, Tiffany Li, "Humans forget, machines remember: Artificial Intelligence and the Right to Be Forgotten" (2018) 34 Computer Law and Security Review 304, 309
[171] ibid.
[172] ibid.
[173] ibid.
[174] ibid.
[175] Michael Veale, Reuben Binns, Lilian Edwards, "Algorithms that remember model inversion attacks and data protection law" [2018] Phil. Trans. R. Soc. 1, 9

means, that even though the personal data might be deleted in the future, it is questionable whether the patterns learnt from data will change according to this. This might not be problematic considering the amount of data that has to be processed for learning purposes. Nevertheless, there might be a need for enhanced testing after big portions of data are deleted. Training the model with new data sets again might become necessary to avoid inaccurate results and avoid biases based on previously learned data. Appropriate processes, however, can only be established after the effective deletion of personal data from AI tools is made feasible. Research shows, that there are possibilities of making deletion of data from AI models more feasible that still require further development.[176]

It can be concluded from the above mentioned, that the principle of storage limitation so far lacks feasibility. The possibility to delete data is not only important for the storage limitation, but also for the right to be forgotten[177] in the GDPR. This is highly problematic since the storage limitation serves an important purpose. It aims at ensuring that data about a data subject cannot be held forever. This is important in times were data breaches as well as changing abilities of controllers and possible uses of data can occur. In fact, it is argued that the storage limitation is crucial when it comes to privacy protection and research on the matter should be much more discussed and furthered within the development of AI.

1.6. Purpose limitation

The purpose limitation as laid down in Article 5 GDPR is an integral principle of processing. It states that personal data shall be collected for specified, explicit and legitimate purposes and shall not be further processed in a manner that is not compatible with the initial purposes.

---

[176] Michèle Finck, "The Limits of the GDPR in the personalisation context" Max Planck Institute for Innovation and Competition Research Paper no 21-11, 8 ,<https://ssrn.com/abstract=3830304> last accessed 11 May 2021

[177] Article 17 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1

While it is alleged in literature that the purpose limitation can harm technological innovation, without this principle the initially collected data could be used for any purpose and be used as many times as the controller wants.[178] This could end up in data being collected for personalized advertisement to be used in assessing the eligibility of a data subject to insurance or similar. Another potential problem is the potential of unintended or not planned outcomes of AI.[179] It is also mentioned that the use of big data in this context leads to an unfair responsibility of the controller to monitor the processing and to make sure the purposes are not exceeded. While it is alleged that this is costly and difficult or even impossible, this argument is highly disputable. Firstly, the controller should be aware of the output of the AI tool anyways. Secondly, AI needs constant testing to assure the accuracy of the decisions or output. Thirdly, if AI could not be "controlled" in the sense to assure that the processing takes place for a certain purpose, its applicability for real-world scenarios could be questioned anyways.

It was also argued by a scholar beforehand that the purpose limitation is a sign of legislator´s paternalism that undermines the autonomy of data subjects by giving rights to the data subject he or she did not ask for.[180] I propose that this argument cannot be accepted due to two reasons. Firstly, a minimum standard of protection should always be self-evidently given. Secondly, the purpose limitation as a principle of processing merely sets a standard that is manifested in other rules of the GDPR that establish duties of the controller and rights of the data subjects. These rights however will typically require actions from the data subjects, rather than being "provided" to a passive data subject.

---

[178] Article 29 Data Protection Working Party, "Opinion 03/2013 on purpose limitation" (WP203, 2 April 2013), 4

[179] Lilian Mitrou, "Data Protection, Artificial Intelligence and Cognitive Services- Is the General Data Protection Regulation (GDPR) 'Artificial Intelligence-Proof?'" [2019] < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3386914> last accesed 10 December 2020, 1, 20

[180] Tal Z. Zarsky, "Incompatible: The GDPR in the Age of Big Data" (2017) 47 Seton Hall Law Review 995, 1007

Another argument that was brought forward, is the idea that the purpose specification would weaken monopolies in data markets while allowing start-ups to enter and compete.[181] I agree to the point of view that the opposite might be true. [182] While the big established companies that hold a big share of the market already have huge databases, start-ups are unable to gather data on the secondary market and therefore are in a competitive disadvantage. Therefore, it can in fact be argued that this principle enhances the dominant position of a few big techcompanies. However, the problem of unproportionally big players in the market disrupting competition however cannot be seen only when it comes to the data processing principles, but rather is a problem in itself.

When it comes to further use of data, not all new purposes are excluded by the purpose limitation. Article 5 (1)(b) states that processing in the light of the purpose limitation needs to be "not incompatible" with the initial purposes. As stated beforehand, this seems to give the controller some leeway for further processing.[183] At least, a case-by-case analysis will be required for further processing operations.

The repurposing of figures is one of the main features of AI in connection with the use of big data. Big data analytics involve the repurposing of data in unexpected ways to draw conclusions about individuals with oftentimes unexpected[184] or even unwelcomed outcomes.[185] An example for the repurposing of data could be the use of recorded voices by Siri, Alexa, and similar means in order to extract biometric findings.[186]

---

[181] ibid.
[182] ibid.
[183] Article 29 Data Protection Working Party, "Opinion 03/2013 on purpose limitation" (WP203, 2 April 2013), 21
[184] Lilian Mitrou, "Data Protection, Artificial Intelligence and Cognitive Services- Is the General Data Protection Regulation (GDPR) 'Artificial Intelligence-Proof?'" [2019] <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3386914> last accesed 10 December 2020, 1, 20
[185] ibid 44.
[186] ibid 47.

To give guidance for the assessment whether the repurposing is within the limits of the purpose limitation, the Article 29 Working Party proposed a compatibility test that could either be formal or substantive. The former would be a formal assessment comparing the purposes that were initially provided by the controller and the new purposes. The latter would describe an assessment that would identify the new and the original purpose while taking into account the way the data subject would understand the purposes in the light of the context and relationship given.[187] It provides a more flexible, pragmatic and more effective methods that enables the adaption to future developments and also continuous use of appropriate safeguards.[188]

While the purpose limitation does request the controller to evaluate the processing of personal data in relation to the purposes that he wants to achieve, this evaluation does not put unendurable pressure on the controller. It is acknowledged however, that the controller is restricted in certain ways. This does not harm the controllers right to ask for consent anew (where this legal ground was used) if the new processing purposes are incompatible with the purposes the processing of data was based on beforehand.

The purpose limitation, by limiting possibilities of repurposing data processing, is crucial to ensure the data subject's rights. Without this principle, the only limits of repurposing and using data that the data subject gave on a voluntary basis for things the data subject would not agree to, is the extent to which this is profitable for the controller and the technological limit and it has to be assumed that the limits of technology lay far beyond what one would call privacy invasive.

Additionally, the GDPR provides for exceptions when it comes to scientific, historical, and statistical research, and archiving purposes in the public interest. Scientific research is interpreted broadly to include technological

[187] Article 29 Data Protection Working Party, "Opinion 03/2013 on purpose limitation" (WP203, 2 April 2013), 21
[188] ibid 22.

development and demonstration.[189] This gives rise to questions of how the purpose limitation can be circumvented. Technological development is truly problematic when it comes to the use of AI as it could be "developing" itself by virtue of the learning capabilities of the AI. One could therefore argue that when it comes to scientific purposes, it will be difficult to distinguish between scientific development and application of AI.[190]

To sum up, the principle of purpose limitation burdens controllers with the duty to foresee the purposes they want to collect and process personal data for before processing and envisioning future purposes to inform the data subjects. The difficulty lies in the fact that it is AI to draw inferences, repurpose data and provide a certain level of "surprise" when it comes to its learning processes. However, this principle should lead the way for development in the field of AI and not be abandoned.

1.7. Conclusion

So far, I have examined the first stages of personalisation including the gathering of data and its legal bases, and the use of this data to derive more knowledge about individuals to improve targeting of advertisement. During this examination, it became clear that consent as a legal ground for processing is highly problematic. In fact, the ideological base for consent and the GDPR as a whole seem to clash with the ideological base of Surveillance Capitalism. This inherent tension will have to be examined further. However, consent as a legal base is problematic for the data subject as the ability to make an informed decision about one's privacy choices is far more complex and difficult than what would be imagined. Examples I gave beforehand stem from the information overflow that data subjects face and power imbalances

---

[189] Lilian Mitrou, "Data Protection, Artificial Intelligence and Cognitive Services- Is the General Data Protection Regulation (GDPR) 'Artificial Intelligence-Proof?'" [2019] <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3386914> last accesed 10 December 2020, 1, 48

[190] Lilian Mitrou, "Data Protection, Artificial Intelligence and Cognitive Services- Is the General Data Protection Regulation (GDPR) 'Artificial Intelligence-Proof?'" [2019] <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3386914> last accesed 10 December 2020, 1, 48

that can lead to the fear of or actual detriment for the data subject. I propose, that in these cases consent should not be used for processing.

Then, I examined profiling itself, meaning the collection of data and its subsequent use for deducing knowledge of individuals. It became clear, that the amount of data that is likely to be collected about data subjects, will oftentimes go beyond what was envisioned when implementing the processing principle of data minimisation. Additionally, profiling raises questions of discriminatory nature that do not face a direct answer from the GDPR.

Additionally, it was shown that the storage limitation so far lacks actual feasibility in the sense that deletion of data from AI models is in its infancy and oftentimes not feasible so far. It will be necessary to encourage further research in the field.

Further, the question of inferences and the connected principle of purpose limitation was explored. There were two important findings. Firstly, by drawing inferences, one generates data that can be personal or sensitive data. Secondly, inferences can reveal unexpected insights about a person and therefore have the potential to infringe the principle of purpose limitation that does indeed limit the amount of purposes to those that the data subject has consented to or where the controller had the legitimate interest and the data subject was informed.

In the following, I will now move to questions of personalisation in the field of news provision.

2. Personalized newsfeed and Propaganda

Controversially, the same social media platforms that are famous for surveillance practices of their users, are also seen to play a role in the spreading of propaganda and disinformation and their contribution to current right trends. Recently, the United Nations Secretary General Antonio Guterres called for international cooperation in battling the spread of white supremacy, propaganda, and disinformation.[191]

The amount of available information is steadily increasing and so does the use of social media for news provision and social interaction.[192] Guterres also mentioned explicitly that the use of social media contributes to the absence of facts in news provision.[193] One could argue that this is an outflow of the attempt of social media to attract attention, or in other words, of Surveillance Capitalism. People like to read what they can establish an emotional connection to, which will typically be confirming their opinion rather than disputing it.[194] This combination of news provision mirroring potentially already existing biases and the possibility to distribute content that might not always be based on facts, can contribute to a fuelled atmosphere spreading widely through societies.

The currently most prominent example that is to mention is the misuse and spread of misinformation and propaganda by former president of the US, Donald Trump. His constant influence and involvement into right-wing ideology that had repeatedly violated social media's hate speech guidelines and advertisement for white supremacy online led to a further rise and spread

---

[191] Al Jazeera, "UN chief urges global alliance to counter rise of neo-Nazis" (26 January 2021) <https://www.aljazeera.com/news/2021/1/26/un-chief-urges-global-alliance-to-counter-rise-of-neo-nazis>, last accessed 28 January 2021

[192] Rasmus Kleis Nielsen, Alessio Cornia, Antonis Kalogeropoulos, "Challenges and Opportunities for news media and journalism in an increasingly digital, mobile and social media environment" (Council of Europe report DGI (206)18) 1, 11

[193] Al Jazeera, "UN chief urges global alliance to counter rise of neo-Nazis" (26 January 2021) <https://www.aljazeera.com/news/2021/1/26/un-chief-urges-global-alliance-to-counter-rise-of-neo-nazis>, last accessed 28 January 2021

[194] Kris Shaffer, *Data versus Democracy, How Big Data Algorithms Shape Opinions and Alter the Course of History*,(apress, 2019), 40

of right-wing ideologies and even caused a mob of his followers to doubt elections and riot in front of the White House.[195]

The personalisation of newsfeeds together with changes in the distribution and reception of propaganda pose significant risks on democracy in many ways. Personalisation of news, despite upsides like the reception of news one is interested in, can lead to the enhancement of biases of a person and have polarisation effects within societies.

A recent example is the misuse of social media and newspapers by the Indian Government. Both the BJP as the leading party under Prime Minister Moodi and the Congress as the Opposition are known for using automated systems for spreading misinformation and propaganda. In fact, in 2019 the BJP made itself a name by spreading propaganda and misinformation for ensuring an electoral win.[196]

As the personalisation of news and propaganda both influence the ability of citizens to inform themselves and take part in the political discourse, in the following, both will be examined. After gaining some understanding of these concepts, the focus will lay on the question of protection. For this reason, firstly questions regarding the processing of special categories of data under the GDPR will be addressed, as well as explicit consent as legal ground for the processing of special categories of data. Lastly, the question will be evaluated whether there is a right to un-personalized information.

2.1. What is a personalized newsfeed?

News personalisation is "a form of user-to-system interactivity that uses a set of technological features to adapt the selection, prioritization, and dissemination of news items to individual users, interests, preferences and

---

[195] Kari Paul, "'Four years of propaganda': Trump social media bans come too late, experts say" <https://www.theguardian.com/us-news/2021/jan/07/donald-trump-facebook-social-media-capitol-attack>, last accessed 3 February 2021

[196] Ualan Campbell-Smith, Samantha Bardshaw, "Global Cyber Troops Country Profile: India", <https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2019/05/India-Profile.pdf>, last accessed 4 February 2021

other personal characteristics".[197] In other words, the personalisation of news works by detecting the interests and preferences of a data subject and monitoring behaviour on the internet and according to this proposing content.

One can differentiate between user driven personalisation and system driven personalisation. The former is based primarily on information that is actively provided by the data subject. An example for that could be the provision of personal information by the data subject and the ticking of boxes indicating favourite news topics or sources.[198] The latter is based on the collection of page views, search history, clicks and likes by a personalisation system to infer or predict someone´s interests.[199] It is proposed that this form of personalisation is more invasive, as the data subject will not necessarily be aware of the amount of data that is collected to infer knowledge about the data subject.

Additionally, the trend goes to reading the news on mobile phones. Mobile apps in general collect more personal data than browser-based applications and therefore create a bigger risk for the data subject.[200] Also, the channels of news consumption changed. While beforehand, traditional newspapers providing online content were the main source of information, people nowadays often turn to social media platforms for news provision.[201] In fact, it was found in a study in 2018 that was conducted across 37 markets, that 45% of respondents named online news as their main source of news consumption. Out of these only one third arrived at online news by directly accessing apps or website of news publishers.[202]

---

[197] Sarah Eskens, "A right to reset your user profile and more: GDPR-rights for personalized news consumers (2019) 9 International Data Privacy Law 153, 155
[198] ibid.
[199] ibid.
[200] ibid 154.
[201] ibid.
[202] Rasmus Kleis Nielsen, Richard Fletcher, " Democratic Creative Destruction? The Effect of a changing Main Landscape on Democracy" in Nathaniel Persily, Joshua A. Tucker (eds) *Social Media and Democracy- The state of the field, Prospects for Reform* (Cambridge University Press, 2020) 149

The purposes of using personalized news are manifold. The controller can aim at showing the diversity of content, trying to push important stories that did not reach enough people or serve niche audiences with specific interests. Additionally, the news provider can aim at enhancing the pay-per-article sales or attempt to provide more context to news events.[203] The use of a personalized newsfeed has several benefits. Information is not a rare good anymore, but instead there is sheer endless information available, finding the relevant information can be difficult. Paying attention to political, economic, and other news is an integral part of a working democracy. The right to be informed therefore would be the basis for a citizen to make choices in elections and everyday life. This was paid tribute in the Charter that explicitly states that there is a right to receive and impart information in article 11 of the Charter.

AI will oftentimes be used in the context of personalization. Personalisation can be automated so that more data can be collected and subsequently be used more meaningfully. Another advancement through AI is that dynamic customer profiles can be made that would adapt campaigns in real time to the needs of the customer.[204] The news selection will be based on demographic details, geolocation, time zone, news stories read, website sections visited, the device type and others.[205]

On one side it is to mention that to a certain extent, the consumer will have an interest in targeted advertisement or information. On the other side, when it comes to political information, targeted information providing can be dangerous and non-beneficial for the consumer. It was argued in literature that news consumption by means of technology can enhance polarization within societies. Additionally, the option of sharing information without

---

[203] Sarah Eskens, "A right to reset your user profile and more: GDPR-rights for personalized news consumers (2019) 9 International Data Privacy Law 153, 162
[204] Leah Fainchtain, "AI Algorithms Are Changing Personalization: Here's How" (2020), <https://developer.ibm.com/recipes/tutorials/ai-algorithms-are-changing-personalization-heres-how/>, last accessed 5 February 2021
[205] Sarah Eskens, "A right to reset your user profile and more: GDPR-rights for personalized news consumers (2019) 9 International Data Privacy Law 153, 153

examining sources is easy in social networks and contributes to a fast distribution of content. This combination of news provision mirroring potentially already existing biases and the possibility to distribute content that might not always be based on facts, can contribute to a fuelled atmosphere spreading widely through societies.

It is proposed that digital technologies facilitate the forming of groups consisting of like-minded individuals that can be increasingly isolated from any challenging information. This process is exacerbated by filtering algorithms.[206] This explanation makes sense in so far, that the use personalisation together with more frequent use of social media for news consumption lead to a filter bubble – the individual is only confronted with views that confirm his or her believes and therefore further their believe in being right in their opinion. It was also shown that individuals tend to become more extreme in their opinion when being confronted with constant confirmation of their opinion by others.[207]

One could argue that the employment of AI carries the risk of AI being able to reinforce certain biases and abuse this position for political and other purposes. While one could argue, that there is many ways in which people with a certain political opinion can ensure to not be confronted with the arguments of the political opposition, the threatening part of this is the fact, that in the case of AI this can happen without the person being aware of the other side. It is to be said however, that it might not be law that has to react to this reinforcement of biases, but rather education. Education in the field of technology as well as in the field of psychology, meaning in this case self-perception and how one forms opinions, could make people better aware of their own biases and more alerted when it comes to the use of technology.

The current right-trend of the European societies as well as cases of propaganda and targeted and personalized political advertisement to

---

[206] Pablo Barberá, "Social Media, Echo Chambers and Political Polarization" in Nathaniel Persily, Joshua A. Tucker (eds), "*Social Media and Democracy, The state of the Field and Prospects for reform"* (Cambridge University Press, 2020), 36
[207] ibid 37.

influence election results display a critical development within the democratic sphere of our society. Although a paternalistic treatment from the state cannot be necessarily wished for, it could be necessary to ensure fairness and protection of citizens through limiting the possibilities of targeting political information and advertisement. The key in fact is, that it is political advertisement. While usual news provision could be balanced by individuals themselves with the right amount of education about the workings of AI, I propose that the field of political advertisement is especially dangerous for data subjects because it combines the knowledge of what an individual wants to hear together with the possibility to deliver this content in the form of an advertisement and can lead to undue influence on political decisions by data subjects.

Before examining whether there is protection available for personalized newsfeeds, I will introduce Propaganda as a topic that should be considered here as propaganda will in fact oftentimes be targeted.

2.2. What is Propaganda?

Especially, when it comes to political advertisement, there are several risks arising that can be result of abusing the possibilities of AI. As seen in Cambridge Analytica, using the detecting abilities of AI can result in abusing vulnerabilities to influence the election behaviour or the general opinion of data subjects.[208]

Propaganda, even though an old phenomenon, becomes magnified in the digital age.[209] The shift from traditional newspapers towards social media, their excessive use also as main source of information means that propaganda is no longer only spread by an entity or organization, the traditional definition

---

[208] Carole Cadwalladr, Emma Graham-Harrison, "Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach", <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>, last accessed 19 November 2020

[209] Johann Farkas, Jannick Schou, Christina Neumayer, "Cloaked Facebook pages: Exploring fake islamist propaganda in social media" (2018) 20 new media & society 1850, 1853

of propaganda suggests, but rather every participant can become spreaders of propaganda through sharing it on social media platforms.[210]

In his book "Data versus democracy", Kris Shaffer proposed the following definition of propaganda: Propaganda is the "use of one or more media to communicate a message, with the aim of changing someone's mind or actions via psychological manipulation rather than reasoned discourse".[211] The messages conveyed present non-facts as facts, incomplete content or content that is stripped of its original context. Propaganda can therefore involve disinformation, as a purposeful attempt to deceive or manipulate and misinformation, an unintentional spreading of falsehood and fallacies.[212]

This definition takes into account the current use of social media platforms like Facebook to spread propaganda not only from an organized group or a state but also by participants within social media that oftentimes, without cross-checking the information received, share the propaganda and therefore help spreading it.[213] In fact, this is an important change that comes with the news consumption through social media. Those data subjects that are targeted with Propaganda, are the ones that, oftentimes unintentionally, contribute to further spreading the messages.

Evidently, the change from traditional journalism to social media also has an impact on propaganda. In fact, it was proposed in literature that consumption of news through social media platforms also changes the way one perceives news.[214] This means, that social media being designed for social interactions in the first place face a relaxed posture from the individual consuming it. Together with the various mixtures of content, the individual might not be as conscious and critical as he or she would be when consuming the news from

---

[210] Kris Shaffer, *Data versus Democracy, How Big Data Algorithms Shape Opinions and Alter the Course of History*,(apress, 2019) 16
[211] ibid.
[212] ibid.
[213] ibid.
[214] ibid 42.

a newspaper.[215] Critically, it was also found that data subjects judge the truthfulness of the content they encounter according to the person who shared the content.[216] While this is not surprising, it will be necassry to sensibilise data subjects for examining the sources of posts and assess their reliability.

Propaganda could go without social media. The "but" lies in the fact that propaganda containing a certain message can nowadays be targeted directly to people that are especially vulnerable to it and can be spread more easily through manipulation and the mentioned resharing of the people targeted initially with the Propaganda. This is facilitated by AI. As AI arguably has the potential of enhancing the effectiveness and increasing the audience of propaganda while lowering the costs,[217] I propose that special protection is needed.

An example for this was seen in Denmark in 2015. In this time, fake islamist Facebook accounts occurred that shared content that was directed against Danes and Denmark.[218] The posts contained clear us/ them constructions that were to separate Danes from Muslims as opposed but internally homogenous groups.[219] As over 72,4 % of all Danes had a Facebook account in 2015, political issues spread rapidly on Facebook. This again, emphasizes the importance of social media in news provision nowadays and the influence on political discussion. Even though the authorship of these profiles was questioned early on, most Facebook users sharing these posts assumed the authors of these posts were in fact radical islamists.[220] The reactions to the posts mostly displayed hatred against the Muslim community as well as general opposition to immigration and oftentimes displayed support for the

---

[215] Kris Shaffer, *Data versus Democracy, How Big Data Algorithms Shape Opinions and Alter the Course of History*,(apress, 2019) 42
[216] ibid 42.
[217] Irina Lock, Ramona Ludolph, "Organizational propaganda on the internet: A systematic review" (2020) 9 Public Relations Inquiry 103, 107
[218] Johann Farkas, Jannick schou, Christina Neumayer, "Cloaked Facebook pages: Exploring fake islamist propaganda in social media" (2018) 20 new media & society 1850, 1852
[219] ibid 1860.
[220] ibid 1852.

right-wing populist Danish People's Party.[221] One account that was called Mehmet Dawah Aydemir was shared 4954 times.[222] Importantly, these fake accounts used the infrastructure of Facebook for spreading their propaganda by deleting comments that questioned the authorship of the profiles.[223]

Interestingly, it could also be argued that while the use of AI enables the special targeting of propaganda, it could also be used to detect propaganda and limit its use. This is especially interesting in the sense that the mere possibility of using AI to limit the harm of the use of AI for targeted news providing could establish a similarly effective remedy to potentially harmful effects.

The GDPR provides no safeguards from propaganda or political advertisement itself, but it does provide special protection for special categories of data, which the political opinion of a data subject belongs to. In general, the processing of sensitive data is prohibited unless one of the exceptions can be applied. In fact, the absence of protection from political advertisement and propaganda here is not a surprise as the initial aim of data protection laws will be to give information control to the data subject. That this information can be used to target or even manipulate individuals into certain political directions is not an aim of data protection laws. Therefore, after examining the level of protection from the GDPR for the processing of special categories of data, the question will arise whether the Charter could be of help here.

2.3. Personalized newsfeed and the journalistic exemption

When it comes to the application of the GDPR, the first question to be raised, is whether the journalistic exemption laid down in article 85 (1) GDPR applies to the personalisation of newsfeeds. Article 85 (1) states that Member States are to reconcile the right to protection of personal data with the right to

---

[221] Johann Farkas, Jannick schou, Christina Neumayer, "Cloaked Facebook pages: Exploring fake islamist propaganda in social media" (2018) 20 new media & society 1850, 1861.
[222] ibid 1857.
[223] Ibid 1861.

freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic, or literary expression. In other words, the article obliges Member States to provide for exemptions for journalistic purposes.

Journalism is in fact a vital part of democracy. Therefore it is not surprising that recital 153 states that the processing of personal data solely for journalistic purposes should be subject to exemptions and derogations from certain provisions of the Regulation if it is necessary to reconcile the right to the protection of personal data with the right to freedom of expression and information as laid down in article 11 of the Charter. It further states that as freedom of expression is of great importance in any democratic society, it is necessary to interpret the notion of journalism broadly.[224]

An example hereto can be found in Dutch and German law implementing article 85 GDWhen it comes to journalistic, artistic or literary works, the data subjects do not have the right to withdraw consent, rectify or erase personal data, restrict processing or to object to automated decision-making.[225]

The CJEU (Court of Justice of the European Union) in the *Satamedia* case determined that a sole journalistic purpose is fulfilled in cases where the sole object of the activities is the disclosure of information, opinions or ideas to the public.[226] The court also found that for the journalistic purpose the medium which is used to transmit the information is not of importance and there is no prohibition of the objective of profit-making from the side of the controller.[227] In the *Google Spain* case that dealt with a request of removal of results from a search engine, the court found that search engine results do not

---

[224] Recital 153 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1

[225] Sarah Eskens, "A right to reset your user profile and more: GDPR-rights for personalized news consumers" (2019) 9 International Data Privacy Law 153, 157

[226] Case C-73/07 *Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy* [2008], para 62

[227] Case C-73/07 *Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy* [2008], para 61

satisfy the definition of a solely journalistic purpose.[228] This proposes, that the purpose is what matters for determining whether personalized news fall under the journalistic exemption or not and the medium with which this information is transmitted does not have to be taken into account. When thinking of the personalized newsfeeds the purpose is not to create new content for the public or inform the public, it is rather providing a selection of information according to an individual's or group's interests.

The purpose of the journalistic exemption is to enable news providers to use personal data in their publication. News personalisation on the other hand does not need this provision.[229] In fact, the creation of content remains still with traditional journalistic entities or the users of social media (by resharing information). Therefore, there is no creation of content that would justify an exemption that aims at enabling the creation of content entailing the use of personal data. Consequentially, the journalistic exemption cannot be assumed to apply in the case of personalized news provision.

2.4. Processing of special categories of data

Personalized news provision and advertisement is based on the gathering of data and the inferring of information concerning one's political opinions, economic interests, and other information relevant to news. Therefore, I will now turn to examine the processing of special categories of data.

Special category data is data revealing racial or ethnic origin, political opinion, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health, sex life and sexual orientation.[230] One could imagine a case within which AI is able to derive one of these attributes from personal data.

---

[228] Case C-131/12 *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* [2014], para 85

[229] Sarah Eskens, "A right to reset your user profile and more: GDPR-rights for personalized news consumers" (2019) 9 International Data Privacy Law 153, 160

[230] Article 9(1) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1

To give an example: being provided with the location of a person together with information on meeting points and times of political parties or religious groups, AI is likely to derive the political opinion belonging to the political party or religious group. This would even be likely with other patterns, such as searches done on the internet, payments to parties, NGOs, or other institutions.

The same is true for ethnic origin when being provided with shopping habits detecting an affiliation with ethnic shops or certain ethnic clothing. A prominent example for this is Facebook giving advertisers the possibility to exclude certain ethnic groups from their advertisements. Under the category of demographics, the advertiser was able to choose the "ethnic affinity" that was derived from liked posts and pages and allowed the advertiser to exclude these groups.[231]

Problematic is mostly the level of protection that should be given to special categories of data. This type of data deals with the core of the private sphere of a person and therefore earns special respect when being processed.

Article 9 of the GDPR provides that this kind of data shall not be processed. It does nevertheless mandate exceptions. One exception that shall be discussed is explicit consent.

2.5. Explicit Consent

To stay within the explicit consent for a moment, the problem arising with AI could be that special categories of data, as mentioned, can be the outcome of drawing inferences. This means that the data that is fed to the algorithm will typically be personal data, while the output of the algorithm can be special categories data. This also can mean that the controller might not be aware that the output of the AI will be special categories of data and therefore cannot use explicit consent when collecting the data in the first place.

---

[231] Julia Angwin, Terry Parris Jr., "Facebook Lets Advertisers Exclude Users by Race", <https://www.propublica.org/article/facebook-lets-advertisers-exclude-users-by-race>, last accessed 22 December 2020

Explicit consent, as referred to in the GDPR, combines the basic requirements of consent as laid down earlier and adds the requirement of the consent to be explicit in the sense that the consent must be given in an express statement.[232] The Article 29 Working Party proposes that this could be reached by phone conversations providing clear information and ask for specific confirmation of the consent, or by a two stage verification of consent.[233]

I submit that explicit consent is likely to suffer from the same weaknesses as the "ordinary" consent, namely the overuse that overwhelms data subjects, significant power imbalances between the data subject and the controller and possibly missing understanding of the significance of the data processed. Moreover, the problem of control over data, as envisoned for consent, is also valid when thinking of explicit consent. This means, that while the GDPR is aiming at giving the data subject control over, in this case, special categories of data, this control might not be achievable in the context of inherently non transparent actions in surveillance capitalism.

Additionally, to give the concept of explicit consent significance, it would need a noteworthy visible differentiation between the regular and explicit consent. Otherwise, the data subject will not be able to differentiate between these two measures of consent and understand the sensitivity and importance of the decision if he or she wants to consent to processing of special categories of data.

Another persistent problem when applying regular and explicit consent in the field of AI is the withdrawal of consent. The question arises whether it will always be possible to delete or remove all data relating to the data subject from databases and from the "memory" of the AI.[234]

---

[232] Article 29 Working Party," Guidelines on consent under Regulation 2016/679" (WP259, last revised and adopted on 10 April 2018), 18

[233] ibid 10.

[234] Lilian Mitrou, "Data Protection, Artificial Intelligence and Cognitive Services- Is the General Data Protection Regulation (GDPR) 'Artificial Intelligence-Proof?'" [2019] <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3386914>, last accesed 10 December 2020, 1, 40

It becomes evident that explicit consent suffers the same ideological shortcomings as consent under the GDPR. Additionally, the problem of inferences creating special categories of data from personal data seems to be not entirely solved.

2.6.Data Protection by Design

Having had a closer look at the principles of data processing as well as consent under the GDPR when it comes to news provision and advertisement, it becomes clear that many problems do not only arise from the ideological base of the GDPR, but also from technical feasibility of the said principles. Therefore, I will now turn to the concept of data protection by design.

Data Protection by design is implemented into the GDPR in article 25. While many papers argue that this provision might give salvation to the mistreatment of data processing principles and data subject´s privacy in general, it is to highlight, that the provision itself has caught a lot of criticism due to its vagueness[235] and the fact that it overlaps with other accountability provisions.[236] Also, apart from pseudonymization, the provision fails to propose specific privacy engineering methods.

In fact, article 25 states that, the controller shall implement appropriate technical and organisational measures that are designed to implement data protection principles and necessary safeguards into the processing to meet the Regulation's requirements and the data subject's rights. The controller is to this by taking into account "the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing".[237]

---

[235] Ira S. Rubinstein, Nathaniel Good, "The trouble with article 25 (and how to fix it): the future of data protection by design and default" (2020) 10 International Data Privacy Law 37, 38

[236] ibid 39.

[237] Article 25 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1

The controller is required to implement "appropriate technical and organisational measures [..] and safeguards into the processing". This again, raises questions. Recital 78 states, that such measures could be the minimisation of processing of personal data, pseudonymising personal data, transparency, and the "enabling" of monitoring by the data subject and "enabling" the controller to create and improve security features.

Firstly, the mentioning of the measure of pseudonymisation as a technical measure was criticised in literature.[238] This is due to the fact that pseudonymized data is less secure as protection than anonymized data.[239]

Secondly, it is to question what enabling in the context of monitoring by the data subject and the controller´s duty to create security features means. This again, lacks clarity and additional value. The GDPR does already stipulate the access rights of the data subject as well as duties of the controller, such as the duty to inform the data subject and to implement appropriate safeguards.

The actual "new" about the data protection by design approach, therefore, seems to be not new at all. Nevertheless, the significance of this provision mostly lays in the fact, that this is the only time that "design" is mentioned in the GDPR.[240] It therefore suggests, that it is rather the engineering itself that should follow the principles of processing and other provisions within the GDPR already and make data protection per se feasible. Would the principles of processing indeed be the base for planning and engineering of models, research in the field of AI and development could be led into a privacy-affirmative direction that is not dependent on voluntary adherence but a duty that can be enforced and would otherwise lead to incompatibility with the GDPR.

Therefore, I propose that the provision of data protection by design could indeed further the protection of data subjects and democracy in mandating a

---

[238] Ira S. Rubinstein, Nathaniel Good, "The trouble with article 25 (and how to fix it): the future of data protection by design and default" (2020) 10 International Data Privacy Law 37, 39
[239] ibid 41.
[240] Ibid.

duty for the controller to implement privacy affirmative design into AI models, if the provision will be clarified and strengthened in the future. In this case, principles of data minimisation, purpose limitation and storage limitation could also be implemented into the AI tool and their feasibility could be re-evaluated. The outcomes of this however will be dependent on the measures taken to implement the provision and most and foremost on the way of implementation of the processing principles. I propose, that it is unlikely that the GDPR will take a radical enough stand to force companies to implement article 25 in a beneficial manner.

2.7. Conclusion

Having examined personalized news provision, it becomes clear that the personalisation can act as a navigation aid through information for data subjects, but also bears risks of being too privacy invasive and provide one-sided information. It was also shown, that it is unlikely, that the journalistic exemption applies to the field of persoanlized news provision as new content is not provided, but rather the content is filtered in a personalized way.

The data that is used and inferred to detect interests and preferences of data subjects can be invasive and belong to the realm of special categories of data. While the GDPR gives a general prohibition of processing of special categories of data, there are exemptions to this rule. The exception that was examined in the context was explicit consent. It was found, that explicit consent is likely to suffer from similar weaknesses as consent and therefore might not be a valuable ground for processing.

Propaganda as an old phenomenon that found its way into the digital age was also examined shortly in the context. Most importantly here is that the main source of news provision are social networks that ease the way to information that is not checked properly and oftentimes disguise the source of origin of the content.

Lastly, the concept of data protection by design was examined to understand, whether this norm could help overcome weaknesses when it comes to ideological clashes between surveillance capitalism and the GDPR.

Unfortunately, this norm is very vague and so far lacks clear interpretations. It seems unlikely that this will be done in the future.

To see whether there is additional protection from the Charter I will now turn to the right to receive and impart information.

3. Is there a fundamental right to receive unbiased information?

As the protection given for personalisation in the field of news provision seems to lack under the GDPR, I will now turn to discuss the question whether the fundamental right to receive and impart information in article 11 in the Charter[241] includes a right to receive unbiased, or unpersonalized information.

When AI is used for tracking data subject's behaviour and deduce a certain information that falls under the realm of special categories of data, one must consider the proficiency and danger arising with the use of AI. Considering the type of data that fall under special categories of data, several harms can be caused, ranging from harms concerning the physical or economic situation of the data subject and harms belonging to the intellectual, social and identity of a person.[242] The potential gravity of these harms justifies a special treatment and protection. It is important to make sure that AI is not used to the detriment of the data subject. Especially when it comes to the right to receive and impart information, one must think of the consequences the use of targeted information providing could have.

In the case of Cambridge Analytica, it became clear that the company had used personal information without authorisation to personalize political advertisements to manipulate the political outcome in the favour of Donald Trump.[243] Later on, it was revealed, that the case of the US election was indeed not an abnormality. Rather, a leak in Cambridge Analytica´s data revealed that the company was working in 68 countries, aiming at election manipulation on an industrial scale.[244] This displays a problem that could

---

[241] Charter of Fundamental Rights of the European Union: 2010 O.J. (C83) 389. Proclaimed by the Commission, 7 December 2000. Proclamation and text at 2000 O.J. (C364)
[242] Damian Clifford, Megan Richardson, Norman Witzleb, "Artificial Intelligence and Sensitive Inferences: New Challenges for Data Protection" ANU College of Law Research Paper No. 21.1, 13-14, <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3754037> , last accessed 12 May 2021
[243] Carole Gadwalladr, Emma Graham-Harrison, "Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach", <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>, last accessed 19 November 2020
[244] Carole Cadwalladr, "Fresh Cambridge Analytica leak 'shows global manipulation is out of control'", <https://www.theguardian.com/uk-news/2020/jan/04/cambridge-analytica-data-leak-global-election-manipulation>, last accessed 19 November 2020

become crucial in the future: Democracy is based on informed citizens that are enabled to make a choice for their political wishes based on the information they are given. Citizens are potentially fed with wrong or misleading information that is intentionally targeted at influencing their political opinions, will not be able to make a free decision on their political will. Additionally, it is questionable if data subjects are informed enough to be able to protect themselves against personalisation, ads, and propaganda that wilfully targets the emotions of data subjects to mislead them. Therefore, it is proposed that there needs to be an additional protection from manipulation for data subjects.

While one could argue that propaganda and personalisation are nothing new, it is to consider that AI due to its characteristics does not only increase efficiency, accuracy, and the amount of data to be evaluated but also provides all these improvements in a hidden space and can arguably pose threats through unnoticed biases.

It can be argued that a personalized newsfeed gives the base of analysis that is necessary to understand the political opinion of an individual. This processing per se might not be a problem, even though it is to mention that a personalisation of the newsfeed bears the risk of giving a one-sided picture which, together with the enhanced use of social media for political discourse, can lead to the enhancing of biases in the data subject rather than an informative provision of latest events and also influence political opinions. As seen in Cambridge Analytica, democracy is at stake when the knowledge of political preferences is abused for targeting special campaigns at a group of people that is likely to believe the campaign and therefore change their voting behaviour.

The right to receive and impart information could be a right to help the data subject here. The roots of the right to receive and impart information has many aspects and finds justification in many parts of democratic societies. While the classical view is the freedom to express one´s opinion freely and not be hindered by authorities, the right also includes the idea of receiving information freely. This is expressively important when thinking of the workings of democracy. Not only is information necessary to build one´s own

political opinions, it also a part of truth finding, avoidance of censorship, personal- and social development, and promotes progress.[245] The right to receive information does not only concern state authorities but is important for all aspects of daily life. Information is the base of education and preserving and enabling education and the forming of opinions is crucial to everybody in a democratic society. The Universal declaration on Human Rights[246] nominates it in article 19, and information rights are implemented in many parts all over the world. Within the EU the right to receive and impart information is laid down in article 11 of the Charter and in article 10 of the European Convention on Human Rights[247].

Article 52 (3) of the Charter states that as long as rights laid down in it have a corresponding right in the Convention for the Protection of Human Rights, those rights shall be the same as laid down in the Convention.[248] The European Convention on Human Rights states in article 10 (1) that "everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers".

An arising problem the European Court of Human Rights (ECtHR) addressed, was the question whether the means of transmission and reception of communication are included in the right to information. It affirmed, that the right to receive and impart information also covers the means of transmission and reception of communication and information.[249] Human Rights are traditionally targeted at states and do not act as horizontal rights, but rather

---

[245] Sarah Eskens, Natali Helberger, Judith Moeller, "Challenged by news personalization: five perspectives on the right to receive information" (2017) 9 Journal of Media Law 259, 261

[246] Universal Declaration of Human Rights (adopted 10 December 1948 UNGA Res 217 A(III) (UDHR)

[247] Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) (ECHR)

[248] Charter of Fundamental Rights of the European Union: 2010 O.J. (C83) 389. Proclaimed by the Commission, 7 December 2000. Proclamation and text at 2000 O.J. (C364) 1 art 52 (3)

[249] *Autronic AG v Switzerland* (1990) Series A no 178, para 47; *Ahmet Yıldırım v Turkey* App no. 3111/10 (ECtHR, 18 December 2012), para 50; *Magyar Ke´tfarku´ Kutya Pa´rt v* Hungary App no 201/17 (ECtHR, 23 January 2018), para 36.

act as vertical rights, meaning that these rights only rule on the relationship between the state and citizens.[250] Nevertheless, the ECtHR, supported in view by policymakers and scholars[251], found in multiple cases[252] that states do have a positive obligation to enable the free flow of information and therefore might be obliged to ensure that users receive balanced news.[253] Additionally, the ECtHR found in the *Dink* case, that states have a positive obligation to create a favourable environment to enable the participation in public debate by all.[254] It also confirmed that states to have a duty to ensure positive protection in the sphere between individuals.[255]

In fact, paragraph two of article 11 of the Charter explicitly refers to an obligation to respect the pluralism of the media. Whether this can be interpreted as also an active obligation to further media pluralism is not decided yet. I propose that the essence of the right is to ensure the freedom of receiving news that allow the data subject to form an opinion freely based on appropriate and diverse information. In case the court would follow this view, the question however would be whether personalized newsfeeds would harm this. Here, I propose that the emphasize again should be on knowledge and freedom. Data subjects are unlikely to be able to make a decision that is based on a conscious choice about not only privacy, but also the consequences for the content of news. This would put the obligation to establish new rules for social media platforms and other actors on the States that did not show much willingness to rule on these actors yet. Additionally, creating domestic laws instead on EU or better international law might only have a limited effect on

---

[250] Sarah Eskens, Natali Helberger, Judith Moeller, "Challenged by news personalization: five perspectives on the right to receive information", (2017) 9 Journal of Media Law 259, 262
[251] ibid 263.
[252] App no. 39293/98 *Fuentes Bobo v Spain (*ECtHR, 29 February 2000), para 38; App no. 23144/93 *Özgür Gündem v. Turkey* (ECtHR,16 March 2000), para 42-43
[253] Sarah Eskens, Natali Helberger, Judith Moeller, "Challenged by news personalization: five perspectives on the right to receive information" (2017) 9 Journal of Media Law 259, 262
[254] ibid 263.
[255] ibid.

big players and would again create legal uncertainty. The form of these laws and the level of protection is also uncertain.

Importantly, this raises the question how balanced or less personalized news could look like. It could be that personalisation itself should be abandoned, or rather that certain personalisation methods or the extent of personalisation needs to be reduced. As it would not necessarily be to the benefit of the data subject to abandon personalisation as a whole, I propose that there should be a limitation to which extend personalisation, and with this the collection and use of data, can take place. I propose that a prohibition of inferring special categories of data together with a prohibition of targeting and inferring data about the mental state of a person would be able to prevent much harm and still enable personalisation. In fact, the regulation on big data and privacy through limitation of inferences that can be used was also proposed by the White House Council of advisors on Science and Technology.[256]

While the ECtHR could acknowledge an obligation for states to implement a right to balanced information and therefore force states to legislate on the use of personalisation derived from the right to receive and impart information in the future, there is no apparent indication so far that this approach would be supported wide enough to be adopted in the future.

Problematic about this approach however is the level of unpredictability of AI. As AI models mostly act like black boxes, it will be difficult to ensure that certain inferences are not made. It is to mention however that there are attempts made to solve the black box problem of AI already. Testing of outcomes according to changes in the input data is one of them. The principle seems easy in the first place- AI is tested for biases by changing one attribute in a data set and noting the change in the output. One could imagine AI deciding on whether an employee is fit for a certain job. If the birthdate is removed and the outcome changes from “no fit” to “fit”, it could show a discrimination of elderly jobseekers. The same could be done with the

[256] A. Sheri, B. Pan, “Get to know me: protecting Privacy and autonomy under big data´s penetrating gaze” (2016) 30 Harvard Journal of Law and Technology 240, 250

nationality of an applicant and so forth. Testing of inferences could be similarly tested by removing certain information in the input data and looking at insights the AI has gained in the output data.[257]

4. EU Proposal for the Artificial Intelligence Act

On 21 April 2021, the European Comission proposed the "Regulation of the European Parliament and of the council laying down harmonised rules on Artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts".[258] While so far this is a proposal only, the present proposal earns some attention in the context of this paper. When explaining the reasons for the proposal, reference is made explicitly to the promotion of trust in AI while addressing risks associated with AI applications.[259] Interestingly, the vast majority of norms laid down in the proposed regulation aim at high-risk AI systems as defined in article 6. Article 6 refers to Annex II and Annex III listing the EU regulations that cover high-risk AI systems. The GDPR however is not referred to in the Annexes.

Article 5 of the proposed regulation however, does give a very limited hope when stating in paragraph (1)(a) that the use and placement in the market of AI systems that deploy techniques to beyond a person's consciousness to distort his or her behaviour in a manner that is likely to cause or cause physical or psychological harm to the person being exposed to it, or a third person, is prohibited. However, this paragraph is very vague, leaving room for questions as to which techniques could be concerned, how this causality would be caused and how the harms would be defined.

Recital 17 gives few guidance. Interesting however is the wording here. "Such AI systems deploy subliminal components individuals cannot perceive or exploit vulnerabilities of children and people due to their age, physical or

---

[257] Ron Schmelzer, "How Do You Test AI Systems?" https://www.forbes.com/sites/cognitiveworld/2020/01/03/how-do-you-test-ai-systems/?sh=74821c57afd5>, last accessed 17 May 2021

[258] Comission, "Proposal for a Regulation Of The European Parliament And Of The Council-Laying Down Harmonised Rules On Artificial Intelligence (Artificial Intelligence Act) And Amending Certain Union Legislative Acts)" COM(2021) 206 final

[259] ibid 1.

mental incapacities. They do so with the intention to materially distort the behaviour of a person and in a manner that causes or is likely to cause harm to that or another person."[260] One can wonder, who has to have an intention to distort the behaviour of data subjects here.

Additionally, it is remarkable that even though personalisation algorithms are undoubtfully used to change the behaviour of persons they are not seen to be high-risk AI systems within the proposed regulation. Rather these systems might find their mentioning in article 5. I propose, that this treatment indicates that problems arising with personalisation are unlikely to be solved, as it seems unlikely that the EU is aiming at prohibiting personalisation all together here. As this however is merely a proposal so far, one could speculate that article 5 (1)(a) has the potential to apply to very invasive practices aiming at the changing of behaviour of data subjects. Whether this harm would already be caused by intrusive marketing that might know one´s interests a little bit "too much", remains to be seen. There might be a chance however, that election advertisements could fall under this norm in the future.

Another interesting point that should be mentioned here is raised in article 55 (1)(a) of the proposed regulation. It obliges Member States to give priority access to AI regulatory sandboxes for small-scale providers and start-ups. Sandboxes are save software test environments.[261] Through this measure, the earlier alleged competitive disadvantages for start-ups in the field of AI could potentially be reduced.

To sum up shortly here, it is to say that the proposed regulation on AI could have an impact on the use of AI when it comes to the willful manipulation of data subjects into detrimental behaviour as well as the competitive disadvantages of start-ups. However, at the moment article 5 is far from being clear and it seems unlikely that personalisation as a whole will be prohibited,

---

[260] Recital 17 Comission, "Proposal for a Regulation Of The European Parliament And Of The Council-Laying Down Harmonised Rules On Artificial Intelligence (Artificial Intelligence Act) And Amending Certain Union Legislative Acts)" COM(2021) 206 final

[261] Eric Geier, "How to Keep Your PC Safe With Sandboxing", <https://www.pcworld.com/article/247416/how_to_keep_your_pc_safe_with_sandboxing.html>, last accessed 17 May 2021

even though personalisation can always have a detrimental impact on the data subject by tricking him or her into a behaviour that harms in or her. It does not have the potential to solve all mentioned problems coming with Surveillance Capitalism however.

IV. Conclusion

The research questions this paper attempts to answer are firstly "What are the effects of AI and Surveillance Capitalism on democracy when it comes to personalisation of advertisement, news provision, and propaganda?" And secondly: "How do the GDPR and the Charter react to these effects and is there still need for additional legislation?"

It was shown that AI in the age of Surveillance Capitalism has the potential to impact democracy in several ways. On an individual level, constant surveillance has the potential to limit the indivudal's space for self-realization and to behave slightly off norms without repercussions. This can lead to data subjects being unwilling to take part in political discourse or otherwise engage into controversial topics.

Surveillance Capitalism proved to have the underlying rationale of circumventing opposition by heavily investing into lobbying and education and acting in opacity. This is one of the reasons data subjects will oftentimes be left without the necessary knowledge and understanding to make decisions in accordance with their privacy preferences when it comes to personalized advertisement and news. It was also shown that personalized advertisement can lead to the revelation of sensitive information about persons and the abuse of this knowledge for economic purposes, namely, to manipulate buying habits to enhance profits. Personalized newsfeeds can have a similar but surely more threatening character when it comes to democracy. The personalisation of news provision can limit the data subject's span of information to one-sided news.

The spread of Propaganda becomes amplified through social media. Additionally, Propaganda can be targeted and therefore be enhanced in its effect. It was found that social media also lead to the fact, that persons being tricked into believing untrue or misleading information are also likely to be the ones sharing this information in a manner that it can deceive others. The factor that is new is the exceptional power of these companies that leads to dangerous influence on society and law-making. It is important to note, that this phenomenon is closely connected to AI. While AI is celebrated and

feared as a revolutionary means, the companies influencing the society´s perception on AI, influencing the law-making are the ones being the drivers of research and development of this technology. The influence on democracy here is evident: Companies should not have the means to influence law-making in a decisive manner and surveillance by companies can lead to the fear of people to take part in open political discourse or even to find information online that could lead to discrimination or is seen to be embarrassing in any way.

To sum up the answer to the first part of the question here, AI influences democracy by using personal data about data subjects in a way that is more than privacy invasive and can lead not only to data subjects being intimidated because of the knowledge of being constantly surveiled, but it also contributes to an environment where the data subject is constantly manipulated into changing his or her behaviour or opinions according to the will of companies. Additionally, it became clear that Surveillance Capitalism, fueled by personalisation of news, advertisements, and propaganda, is designed to operate in an opaque manner to avoid opposition. It also aims at enhancing support from legislators as well as civil societies through heavy investments.

To come to the second part of the question, namely how the GDPR and the Charter react to these effects on democracy, it is to mention that the GDPR, even though technology neutral, does give some sort of relief through access rights as well as the data processing principles of which some where evaluated earlier.

So far, the GDPR however does not live up to the legislative needs for enabling a privacy affirmative application of AI in personalisation. I propose that one reason for the missing protection so far lays in the clash of the underlying rationale of the GDPR and Surveillance Capitalism. The GDPR aims at enabling the data subject to act according to his or her privacy preferences, while Surveillance Capitalism aims at hiding data collection and processing to avoid opposition from data subjects. An upcoming topic is in fact that data subjects lack understandable information, are not informed at all, or cannot easily understand the information given. This is highly

problematic where the legal basis of protection is dependend on this knowledge of the data subject.

In fact, the examined data processing principles seem to be at odds with the current stands of AI oftentimes. While the purpose limitation struggles with the repurposing of data that is seen to be a key feature of AI, the principle of data minimisation is in contrast with the maxime of collecting as much data as possible. The same is true for the principle of storage limitation. It does make sense to oblige controllers to delete data after a certain period, but if this idea simply lacks feasibility, the principle simply looses its value.

Article 25 of the GDPR that obliges the controller to implement the provisions of the GDPR into the design of technology might be the solution to these weaknesses, but so far lacks clarity. It is argued that data protection by design, if adhered to as the obligation to implement privacy affirmative engineering of models into the data processing, might be able to cover a wide range of so far unsolved problems. Nevertheless, this design can only be asked where the research and development on privacy affirmative technologies is concluded and brought about change, such as the possibility to easily delete data from relational databases or AI models in an efficient manner. It remains to be seen if this can be achieved, taking into account that this will not necessarily be in the interest of the economic actors.

The Charter proved to be a valid option for protecting data subjects from privacy invasive practices in personalisation, at least when it comes to the provision of personalized news. This however, would take place through an obligation of member states of the EU to implement measures to ensure the freedom of the data subject to receive unpersonalized information. As this is not an established duty however, it remains to be seen if this obligation will be adopted in the future.

The EU Proposal for the European Artificial Intelligence Act as a potential future regulation proved to be rather disappointing in the context of personalization. Personalisation does not seems to be covered as high-risk system and therefore can only fall under article 5 of the proposed regulation. However, this might be unlikely due to the fact that personalisation per se has

proven to have the potential to manipulate data subjects into unbeneficial behaviour and would therefore have to be prohibited completely. I do not see any indications that would support the view that this is in the interest of the European Union.

"In any complex and chaotic system, including AI systems, potential dangers include mismanagement, design vulnerabilities, accidents, and unforeseen occurrences". [262] As AI is a driving force of Surveillance Capitalism, I propose that upcoming laws aiming at filling the gaps left by the GDPR should follow the rationale of chaos and the regularities of Surveillance Capitalism to respond appropriately to privacy risks and safeguard privacy better.

[262] World Economic Forum, <http://reports.weforum.org/global-risks-2017/part-3-emerging-technologies/3-2-assessing-the-risk-of-artificial-intelligence/>, last accessed 5 December 2020

V. Bibliography

Cases

- *Ahmet Yıldırım v Turkey* ECHR 2012-VI
- *Autronic AG v Switzerland* (1990) Series A no 178
- Case C-131/12 *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* [2014]
- Case C-524/06 *Heinz Huber v Bundesrepublik Deutschland*; [2008]
- Case C-73/07 *Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy* [2008]
- *Fuentes Bobo v Spain no. no. 39293/98 (*ECtHR,29 February 2000)
- *Magyar Ke´tfarku´ Kutya Pa´rt v* Hungary App no 201/17 (ECtHR, 23 January 2018)
- *Özgür Gündem v. Turkey*, no. 23144/93 (ECtHR,16 March 2000)

Books

- Bygrave L, *Data Protection Law, Approaching its Rationale, Logic, and Limits,* (Kluwer Law international, 2002) 128
- Djeffal C, "AI, Demcracy and the Law" in Andreas Sudmann(ed), *The Democratization of Artifcial Intelligence- Net Politcs in the Era of Learning Algorithms* (transcript Verlag, 2019)
- Knuth D, *Fundamental Algorithms- The Art of Computer Programming* (2nd edn, Addison -Wesley Publishing Company, 1973)
- Naudts L, "How Machine Learning Generates unfair inequalities and how data protection instruments may help in Mitigating Them" in Ronald Leenes, Rosamunde van Brakel, Serge Gutwirth, Paul de Hert (ed), *Data Protection and Privacy, the Internet of Bodies* (Oxford: Hart Publishing 2018) 76
- Nielsen R; Fletcher R, "Democratic Creative Destruction? The Effect of a changing Main Landscape on Democracy", in Nathaniel

Persily, Joshua A. Tucker (eds) *Social Media and Democracy- The state of the field, Prospects for Reform* (Cambridge University Press, 2020)

- Schmertzing L, "Democracy in the Age of Artificial intelligence" in Danièle Réchard (ed) *Global Trendometer, Essays on medium- and long-term global trends July 2018* (European Parliamentary Research Service, Essays on medium- and longterm global trends, 2018) 16, 17
- Sen A, The Idea of Justice, (Penguin Books, 2010) 229
- Shaffer K*, Data versus Democracy, How Big Data Algorithms Shape Opinions and Alter the Course of History*,(apress, 2019)
- Timan T; Galic M; Koops BJ, "Surveillance Theory and its implications for law" in Roger Brownsword, Eloise Scotford, Karen Yeung (eds) *The Oxford Handbook of Law, regulation, and technology* (Oxford University Press 2017) 737
- Zuboff S, *The Age of Surveillance Capitalism- the Fight for a human future at the new Frontier of Power* (Profile Books, 2019)

Article 29 Working Party

- Article 29 Working Party, "Opinion 15/2011 on the definition of consent" (WP187, 13 July 2011)
- Article 29 Working Party," Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679" (WP251 rev. 01, 3 October 2017)
- Article 29 Working Party,"Guidelines on consent under Regulation 2016/679" (WP259, last revised and adopted on 10 April 2018)
- Article 29 Data Protection Working Party, " Opinion 03/2013 on purpose limitation" (WP203, 2 April 2013)
- Article 29 Working Party "Opinion 06/2014 On the notion of legitimate interests of the data controller under article 7 of Directive 95/46/EC" (WP217, 9 April 2014)

- European Data Protection Board, “Guidelines 05/2020 on consent under Regulation 2016/679”(edpb, 4 May 2020)

Articles

- Aho B; Duffield R, “Beyond surveillance capitalism: Privacy, regulation and big data in europea and China” (2020) 49 Economy and Society 187
- Atikan E; Calmers A, “Choosing lobbying sides: the General Data Protection Regulation of the European Union” (2019) 39 Journal of Public Policy 543, 543
- Barberá P,” Social Media, Echo Chambers and Political Polarization” in Nathaniel Persily, Joshua A. Tucker (eds), “Social Media and Democracy, The state of the Field and Prospects for reform” (Cambridge University Press, 2020), 36
- Bond R; Fariss C; Jones J; Kramer A, Marlow C; Settle J; Fowler James, “A 61-million-person experiment in social influence and political mobilization” (2012) 489 Nature 295, 295
- Christl W, “Corporate Surveillance in Everyday life, How Companies Collect, Combine, Analyzed, Trades and Use personal Data on Billions” (Cracked Labs, June 2017)
- Clifford D; Richardson M; Witzleb N, “Artificial Intelligence and Sensitive Inferences: New Challenges for Data Protection” ANU College of Law Research Paper No.21,1, <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3754037> last accessed 12 May 2021
- De S; Imine A, “Consent for targeted advertising: The case of Facebook” (2020) 35 AI & Society 1055

- Edwards L; Veale M, “Slave to the Algorithm? Why a ‘Right to an Explanation’ is probably not the remedy you are looking for” (2017) 16 (1) Duke Law and Technology Review 18
- Eskens S, “A right to reset your user profile and more: GDPR-rights for personalized news consumers (2019) 9 International Data Privacy Law 15
- Eskens S; Helberger N; Moeller J, “Challenged by news personalisation: five perspectives on the right to receive information” (2017) 9 Journal of Media Law 259
- Farkas J; Schou J; Neumayer C, “Cloaked Facebook pages: Exploring fake islamist propaganda in social media” (2018) 20 new media & society 1850
- Finck M, “The Limits of the GDPR in the personalisation context” Max Planck Institute for Innovation and Competition Research Paper no 21-11, 8 ,<https://ssrn.com/abstract=3830304> last accessed 11 May 2021
- González E; Hert P, “Understanding the legal provision that allow processing and profiling of personal data- analysis of GDPR provisions and principles” [2019] (ERA Forum), 598
- Goyal N; Howlett M; Taeihagh A, “Why and how does the regulation of emerging technologies occur? Explaining the adoption of the EU General Data Protection Regulation using the multiple streams framework” [2021] Regulation & Governance 9
- Graham N; Davies M; Lee Godden, “Broadening law´s context: materiality in socio-legal research” (2017) 26 Griffith Law Review, 481
- Kamarinou D; Millar C; Singh J, “Machine learning with personal data” (Queen Mary University of London, School of Law, Legal Studies Research Paper 247/2016) 1
- Karwatzki S; Dytynko O; Trend M; Veit D, “Beyond the Personalization-Privacy Paradox: Privacy valuation, Transparency

Features, and Service Personalization" (2017) 34 Journal of Management Information Systems 369

- Lock I; Ludolph R, "Organizational propaganda on the internet: A systematic review" (2020) 9 Public Relations Inquiry 103
- Marty F; Warin T, "The use of AI by Online Intermediation Platforms Conciliating Economic Efficiency and ethical Issues" Delphi (2019) 4, 217
- Mitrou L, "Data Protection, Artificial Intelligence and Cognitive Services- Is the General Data Protection Regulation (GDPR) 'Artificial Intelligence-Proof?'" [2019] <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3386914> last accessed 10 December 2020, 1
- Narayanan A; Reisman D, "The Princeton Web Transparency and Accountability Project" [2017] <https://www.cs.princeton.edu/~arvindn/publications/webtap-chapter.pdf>, ast accessed 22 December 2020
- Nielsen R; Cornia A; Kalogeropoulos A, "Challenges and Opportunities for news media and journalism in an increasingly digital, mobile and social media environment" (Council of Europe report DGI (206)18) 1
- Niemitz P, "Constitutional democracy and technology in the age of Artificial Intelligence" [2018] Phil.Trans.R. Soc. 1
- O'Callaghan J, "Inferential Privacy and Artificial Intelligence - A New Frontier? [2018] <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3301354>, last accessed 22 December 2020
- Oijen V; Vrabec H, " Does the GDPR enhance consumers´control over personal data? An analysis from a behavioural perspective" [2019] Journal of Consumer Policy 91
- Pan S, "Get to know me: protecting Privacy and autonomy under big data´s penetrating gaze" (2016) 30 Harvard Journal of Law and Technology 240

- Rubinstein I; Good N, “The trouble with article 25 (and how to fix it): the future of data protection by design and default” (2020) 10 International Data Privacy Law 37
- Samoili et al., “AI Watch Defining Artificial Intelligence Towards an operational definition and taxonomy of artificial intelligence” (Publications Office of the European Union 2020) 12
- Schmertzing L, “Democracy in the Age of Artificial intelligence” (European Parliamentary Research Service, Essays on medium- and longterm global trends, July 2018) 16
- Villaronga E; Kieseberg P; Li T, “Humans forget, machines remember: Artificial Intelligence and the Right to Be Forgotten” (2018) 34 Computer Law and Security Review 304
- Wang P, “On Defining Artificial Intelligence” [2019] Journal of Artificial General intelligence,1
- Yampolskiy R, “Unpredictability of AI: On the impossibility of Accurately Predicting All Actions of A Smarter Agend” (2020) 7 Journal of Artificial Intelligence and Consciousness 109
- Yeung K, “Five Fears about mass predictive personalization in an age of surveillance capitalism” (2018) 8 International Data Privacy 258
- Zarsky T, “Incompatible: The GDPR in the Age of Big Data” (2017) 47 Seton Hall Law Review 995

Websites

- Al Jazeera, “UN chief urges global alliance to counter rise of neo-Nazis” (26 January 2021) <https://www.aljazeera.com/news/2021/1/26/un-chief-urges-global-alliance-to-counter-rise-of-neo-nazis>, last accessed 28 January 2021
- Angwin J; Parris Jr T., “Facebook Lets Advertisers Exclude Users by Race”, <https://www.propublica.org/article/facebook-lets-advertisers-exclude-users-by-race>, last accessed 22 December 2020

- Cadwalladr C, “Fresh Cambridge Analytica leak ‘shows global manipulation is out of control’”, <https://www.theguardian.com/uk-news/2020/jan/04/cambridge-analytica-data-leak-global-election-manipulation>, last accessed 19 November 2020
- Cadwalladr, C; Graham-Harrison E, “Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach”, <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>, last accessed 19 November 2020
- Campbell-Smith U; Bardshaw S, “Global Cyber Troops Country Profile: India”, < https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2019/05/India-Profile.pdf>, last accessed 4 February 2021
- Eric Geier, “How to Keep Your PC Safe With Sandboxing”, <https://www.pcworld.com/article/247416/how_to_keep_your_pc_safe_with_sandboxing.html>, last accessed 17 May 2021
- Fainchtain L, “AI Algorithms Are Changing Personalization: Here's How” (2020), < https://developer.ibm.com/recipes/tutorials/ai-algorithms-are-changing-personalisation-heres-how/>, last accessed 5 Febraury 2021
- Glick M; Ruetschlin C, “Big Tech Acquisitions and the Potential Competition Doctrine: The Case of Facebook” (2019), Institute for New Economic Thinking, <https://www.ineteconomics.org/uploads/papers/WP-104-Glick-and-Reut-Oct-10.pdf>, last accessed 1 February 2021
- Maguire L, “Gen Z is reinventing social media marketing” <https://www.voguebusiness.com/consumers/gen-z-reinventing-social-media-marketing-tiktok-youtube-instagram-louis-vuitton>, last accessed 12 February 2021
- Mishra S, “Unsupervised learning and Data Clustering” (2017) <https://towardsdatascience.com/unsupervised-learning-and-data-clustering-eeecb78b422a> accessed 5 February 2021

- Morgan B, “The 7 Best Examples Of Artificial Intelligence To Improve Personalization”[2019], <https://www.forbes.com/sites/blakemorgan/2019/01/24/the-7-best-examples-of-artificial-intelligence-to-improve-personalisation/?sh=309545a3c4ed>, last accessed 9 November 2020
- Paul K, “'Four years of propaganda': Trump social media bans come too late, experts say” <https://www.theguardian.com/us-news/2021/jan/07/donald-trump-facebook-social-media-capitol-attack>, last accessed 3 February 2021
- Peart A, “Homage to John McCarthy, the father of Artificial Intelligence (AI)” [2020], <https://www.artificial-solutions.com/blog/homage-to-john-mccarthy-the-father-of-artificial-intelligence>, last accessed 4 November 2020
- Privacy International, “Data Is Power: Profiling and Automated Decision-Making in GDPR” [2017] <https://privacyinternational.org/sites/default/files/2018-04/Data%20Is%20Power-Profiling%20and%20Automated%20Decision-Making%20in%20GDPR.pdf>, last accessed 9 February 2021
- Research Priorities for Robust and Beneficial Artificial Intelligence <https://futureoflife.org/ai-open-letter/?cn-reloaded=1>, last accessed 22 December 2020
- Ron Schmelzer, “How Do You Test AI Systems?” https://www.forbes.com/sites/cognitiveworld/2020/01/03/how-do-you-test-ai-systems/?sh=74821c57afd5>, last accessed 17 May 2021
- Russell S; Dewey D; Tegmark M, “Research Priorities for Robust and Beneficial Artificial Intelligence” [2015], <https://futureoflife.org/data/documents/research_priorities.pdf?x96845>, last accessed 10 December 2020

- Russell S; Dewey D; Tegmark M, “Research Priorities for Robust and Beneficial Artificial Intelligence” [2015], <https://futureoflife.org/data/documents/research_priorities.pdf?x96845>, last accessed 10 December 2020
- Savage N, “How AI is improving cancer diagnostics Artificial intelligence can spot subtle patterns that can easily be missed by humans.” <https://www.nature.com/articles/d41586-020-00847-2>, last accessed 3 December 2020
- Speicher T; Ali M; Venkatadri G; Ribeiro F; Arvanitakis G, et al., “Potential for Discrimination in Online Targeted Advertising” [2018] <https://hal.archives-ouvertes.fr/hal-01955343> last accessed 22 December 2020
- Statista, “Advertising Revenue of Google from 2001 to 2020”, https://www.statista.com/statistics/266249/advertising-revenue-of-google/, last accessed 12 February 2021
- Sternberg R; “Human intelligence”, <https://www.britannica.com/science/human-intelligence-psychology>, last accessed 4 November 2020
- Tankovska H, “Facebook: advertising revenue worldwide [2021], < https://www.statista.com/statistics/271258/facebooks-advertising-revenue-worldwide/>, last accessed 12 February 2021
- The World Bank, “Bulgaria”, https://data.worldbank.org/country/BG, last accessed 12 February 2021
- Veale M; Binns R; Edwards L, “Algorithms that remember model inversion attacks and data protection law” [2018] Phil. Trans. R. Soc. 1
- Wolford B, “What is GDPR, the EU’s new data protection law?” <https://gdpr.eu/what-is-gdpr/> last accessed 10 May 2021
- World Economic Forum, <http://reports.weforum.org/global-risks-2017/part-3-emerging-technologies/3-2-assessing-the-risk-of-artificial-intelligence/>, last accessed 5 December 2020