UiO : Faculty of Law
University of Oslo

In what ways do the principles in Art 5 (1)(a) GDPR protect consumers against manipulative online marketing?

Candidate number: 7010

Submission deadline: 16 May 2022

Number of words: 17 976

Table of contents

1 Introduction

1.1 Background and relevance

In this paper I will discuss the three principles in Art 5 (1) (a) of the General Data Protection Regulation[1] (hereby referred to as GDPR) in relation with manipulative online marketing. These three principles are the principles of lawfulness, fairness and transparency. I want to shed light on some aspects of online marketing that can be manipulative towards the data subject (the user/consumer), namely collection of data through websites` use of third-party cookies, and collection of data from social media platforms and how this data is used for targeted advertisments. I want to discuss these practices in relation with said principles, and how the principles can provide protection and be used against this. Since the GDPR regulates the processing of personal data,[2] my focus will be limited to online marketing that involves processing of personal data.

The reasons for discussing this topic is part of a bigger picture. As our societies and our lives are becoming increasingly digitalized, with more and more of our daily activities happening online, we leave behind extensive digital footprintsts of data about ourselves, often "personal data".[3] Some examples of the data being collected is our browsing history, IP-addressess, purchase history and our activities and content on social media platforms.[4] One way some of this data is collected is through the use of cookies.[5] The collection and use of extensive data from users/consumers, has created a new economy that is referred to as surveillance capitalism.[6] The term surveillance capitalism is used to describe *"a new economic order that claims human experience as free raw material for hidden commercial practices of extraction,*

[1] Regulation (EU) 2016/679 of the European Par-liament 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 945/46/EC

[2] Art 2 (1) GDPR

[3] European Data Protection Supervisor (EDPS), Opinon 3/2018 on online manipulation and personal data Page 7-8

[4] European Data Protection Supervisor (EDPS), Opinon 3/2018 on online manipulation and personal data Page 8

[5] European Data Protection Supervisor (EDPS), Opinon 3/2018 on online manipulation and personal data Page 8

[6] Shoshana Zuboff, *The Age of Surveillance Capitalism – The fight for a human future at the new frontier of power* (USA: Profile Books, 2019) page 8

prediction, and sales".[7] The advertising industry is an important commercial practice in this context, which will be the overall topic in this paper.

Enormous amounts of data from online users is collected in order to predict consumer behavior, so that commercial companies can more easily target them in a given market.[8] Targeting is defined as *"the act of attempting to appeal to a person or a group or to influence them in some way"* and as *"the act of directing or aiming something at a particual group of people"*.[9] In the advertising industry, companies want as much information about its potential customers as possible, in order to capitalize on this data by presenting consumers with personalized/targeted advertisements.[10] In pre-internet times the advertisers had to anticipate where they would meet their desired consumers and place their ads there, such as in newspapers or on television, as opposed to today, where advertisers can target their consumer online based on their interests and digital footprint.[11] Instead of hoping that *the consumer would come to where the ad was*, for instance a bus stop, commercial break during a television show, in a feature article in a magazine, now *the advertisements can come to where the consumer is* by keeping track of the consumer`s online life and following them around. That is what you call a game changer.

The rise of surveillance capitalism, including targeting of consumers in the advertising industry, raises many concerns with respect to fundamental rights such as the right to privacy. One concern regards social media platforms in particular, and what is concerning is that social media users are being targeted on the different social media platforms for "commercial, political or

---

[7] Zuboff, *The Age of Surveillance Capitalism – The fight for a human future at the new frontier of power* page 1 (See page headline "The definition")

[8] Kirstie Ball and William Webster «Big Data and surveillance: Hype, commercial logics and new intimate spheres" *Big Data & Society* Volume 7 Issue 1 (2020) page 2

DOI: https://doi.org/10.1177%2F2053951720925853

[9] Collins dictionary "Definition of targeting", access date 4 March 2022 https://www.collinsdictionary.com/dictionary/english/targeting. See also European Data Protection Board Guidelines 8/2020 on the targeting of social media users Version 1.0, page 3

[10] European Data Protection Supervisor (EDPS), Opinon 3/2018 on online manipulation and personal data, Pages 9-10

[11] The Economist, "How Apple`s privacy push cost Meta $10 bn", February 3rd 2022, https://www.economist.com/the-economist-explains/2022/02/03/how-apples-privacy-push-cost-meta-10bn

See also The Norwegian Consumer Counsil`s (Forbrukerrådet) report "Out of control – How consumers are exploited by the online advertising industry" (2020) Page 13 https://fil.forbrukerradet.no/wp-content/uploads/2020/01/2020-01-14-out-of-control-final-version.pdf

other interests".[12] In this paper the focus will be on the commercial aspect, more specifically advertising technology and online marketing. The issue of *manipulation* in connection with online marketing will be discussed both on a general level, but also more specifically in connection with use of third-party cookies and data collection on social media platforms. When discussing manipulation, the term "dark patterns" will also be of relevance. This term is defined as *"...features of interface design crafted to trick users into doing things that they might not want to do, but which benefit businesses in question"*.[13] In a few instances in this paper there will be made some examples of different types of dark patterns, as these are practices that are evident in our daily digital dealings, but the focus will also be on manipulative tendencies without necessarily constituting a dark pattern.

1.2 Research question

Online advertising practices raise serious data protection and privacy issues, which is part of the bigger discussion in this paper. The main focus is the more specific issue of advertising practices that are arguably manipulative in the way the data is collected and subsequently used to target consumers. I will discuss and argue that consumers are often being manipulated when it comes to how data is collected, for instance through use of third-party cookies/tracking cookies or collection of data from social media platforms. I will also look at how the data is concequently used, for instance through targeted advertisments showed in a social media feed or on websites.

This paper will not discuss marketing practices per se. The issue to be discussed, with the lawfulness, fairness and transparency principles set forth in Art 5 (1) (a) GDPR as the legal basis, is *manipulative* marketing online done by commercial actors. There are multiple marketing techniques online that are arguably manipulative that do not necessarily involve processing of personal data, such as misleading text, images and presentation in ads, or how the top of the

[12] See European Data Protection Board Guidelines 8/2020 on the targeting of social media users Version 1.0 page 3

[13] Forbrukerrådet (Norwegian Consumer Counsil), Report "Deceived by design: How tech companies use dark patterns to discourage us from exercising our rights to privacy» (2018), page 7, https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf

Google search list can be bought for ad-placements (they are labelled "ad" with small font) instead of giving the top spots to the most relevant search. Since the discussion is in what ways fundamtental principles in *GDPR* protect against manipulative marketing online, and GDPR only regulates processing of personal data,[14] the focus will be on manipulative techniques/practices that involve processing of personal data.

The main question is how these three principles protect consumers against manipulative uses of their personal data. There are multiple ways to discuss manipulative online marketing in relation with GDPR. I have chosen to focus my discussion around the three said principles. The topic manipulative online marketing is also quite vast and complex, which made it necessary to limit my discussion by focusing on a few selected examples of manipulative practices within online marketing. These chosen examples are meant to give a better understanding of how manipulation can manifest.

I will use examples of manipulative practices that involve processing of personal data and discuss these, namely 1) the use of third party cookies and 2) targeted advertisments based on data collected from social media platforms. One part of the discussion regarding cookies, is the way cookie banners are designed in order to gain your acceptance. Cookies banners informing you of the use of cookies are often designed to make it very easy for a consumer to accept all cookies, but much harder to reject them.[15] It is important to clarify that cookies are also regulated in other legislation, such as the current ePrivacy directive and the proposed ePrivacy regulation that is set to replace the directive.[16] Regarding the discussion on targeted ads directed at social media users, the European Data Protection Board (hereby reffered to as the EDPB) points to the risk that such targeting could lead to/amount to manipulation of social media users.[17] Personal data is collected and used to target users with *presumed* relevant advertisments. The legal basis for this collection is often long and complex user agreements that the user has to agree to in order to use the service.

---

[14] Art 2(1) GDPR states that the regulation "applies to the processing of personal data wholly or partly by automated means(…)".

[15] Miads Nouwens et al "Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence" *Proceedings of the 2020 CHI Conference on human factors in computing systems* (2020) Page 5 https://doi-org.ezproxy.uio.no/10.1145/3313831.3376321

[16] Directive 2002/58/EC (Directive on privacy and electronic communications); see for instance Art 6 (3) and Art 9 (1) requiring consent when processing traffic data and location data other than traffic. See also gdpr.eu, "Cookies, the GDPR, and the ePrivacy Directive" access date 11 May 2022 https://gdpr.eu/cookies/

[17] EDPB Guidelines 8/2020 on the targeting of social media users Verison 1.0, Page 5

I will discuss what constitutes "personal data", and discuss the above mentioned manipulative practices, and see to what degree they are in fact manipulative. In order to do this the term "manipulation" has to be addressed, see chapter 2. In section 2.2.3 and 2.3.4 the two examples are further explained. By using these two examples I demonstrate how our personal data is unwillingly collected and used in ways that is not clear to the user, and damaging to our privacy rights.

"Manipulation" is not a legal term per se, and is not mentioned anywhere in the GDPR. However, it is a fitting term to use in this discussion, given that an important aspect of data protection and privacy law is autonomy/self-determination, and manipulation is the opposite of that.

Marketing can often be based on personal data, especially now in the growing business of big data analytics and online behavioral advertising. Therefore, it is interesting to look more closely at GDPR in this context, since the regulation provides data protection. Manipulative marketing by using personal data raises serious privacy issues, which is why it is relevant to ask the following question, the research question for this paper:

In what ways do the principles in Art 5 (1)(a) GDPR protect consumers against manipulative marketing online?

To be clear, GDPR is not the only legislation that provides consumer protection and data protection in this context. Some important examples of other legislation that provides data protection rights to consumers is the ePrivacy Directive[18] (expected to be replaced by the ePrivacy Regulation[19]), the Directive on Unfair Commercial Practices[20], or the proposed Digital Services

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

[19] COM (2017) 10: Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)

[20] DIRECTIVE 2005/29/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive')

Act[21], where for instance Art 24, Art 30 and Art 36 in the proposal is regarding online advertising.

When discussing "online marketing", it is important to specify what I mean by this term. Firstly, the term "online marketing", or "marketing" for that matter, is not mentioned in the GDPR. There is a similar term, "direct marketing", that is mentioned and regulated in Art 21 GDPR. "Direct marketing" and Art 21 GDPR will be discussed in some detail in relation to targeted ads on social media platforms in the context of the lawfulness principle, see section 3.3.1. For the purpose of the discussion in this paper, I have defined the term "online marketing" in a widely manner: Within the definition I include the advertisments themselves, be it on social media platforms or on a website, but I also include the collection, analyzing and sorting of personal data which are then utilized to create targeted ads, as being part of what defines "online marketing". It is not merely the ad itself (the actual presentation of the product/service) that is defined as online marketing, but also the process leading up to/behind the ad.

The European Data Protection Supervisor (EDPS) points to the fact that online manipulation is often a *"three-stage cycle from data collection (a form of data processing under EU law) through profiling to microtargeting or personalisation as a form of manipulation which can vary in degree from trivial to seriously harmful".*[22]

Such manipulation can also be referred to as "dark patterns". "Dark patterns" is a term that can be described as *"...features of interface design crafted to trick users into doing things that they might not want to do, but which benefit business in question".*[23] The EDPB has recently published new guidelines on the subject of dark patterns on social media platforms, and defines dark patterns as *"interfaces and user experiences implemented on social media platforms that lead users into making unintended, unwilling and potentially harmful decisions regarding the processing of their personal data. Dark patterns aim to influence users' behaviour and can*

[21] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC

[22] EDPS Opinon 3/2018 on online manipulation and personal data page 7

[23] Forbrukerrådet (Norwegian Consumer Counsil), Report "Deceived by design: How tech companies use dark patterns to discourage us from exercising our rights to privacy» (2018), page 7, https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf

hinder their ability to effectively protect their personal data and make conscious choices".[24] So we see from the defintions of the concept "dark patterns", that this is a practice/technuiqe that is manipulative in its nature, and arguably a more severe type/degree of manipulation.

In the following section 1.3, I will give an overview and explanation on the sources and methodology used in this paper.

1.3 Sources and methodology

The main legal source is the GDPR. Within the GDPR, the primary focus is Art 5 (1)(a), but I will also view it in connection with some related articles in the regulation. When interpreting the articles, the recitals of the preamble will be of value. The articles in GDPR do not always give explanations/descriptions on how they are to be interpreted and applied. The recitals in the preamble of the GDPR can be of great interpretative value. As pointed out by Klimas and Vaiciukaite, *"recitals in EC law are not considered to have independent legal value, but they can expand an ambiguous provision's scope".*[25] If a provision is unclear, but a relevant recital is clear, the provision will be interpreted in the light of the recital.[26] Throughout the thesis I will make several references to the recitals, precicely for interpretative value.

In my discussions I apply a variety of legal sources. GDPR is the legal basis, but I have made use of the entire scale of sources, ranging from hard law (mainly the GDPR), to soft law, such as guidelines and opinions from the European Data Protection Board (EDPB) and the Article 29 Data Protection Working Party (The Working Party). The Working Party was given a

[24] EDPB Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognise and avoid them page 2

[25] Klimas, Tadas ; Vaiciukaite, Jurate "The law of recital in European Community legislation" *ILSA journal of international & comparative law*, Vol 15 Issue 1 (2008), page 63 https://heinonline-org.ezproxy.uio.no/HOL/Page?lname=&public=false&collection=journals&handle=hein.journals/ilsaic15&men_hide=false&men_tab=toc&kind=&page=63. See also Frederik J. Zuiderveen Borgesius, "Singling out people without knowing their names – Behavioural target-ing, pseudonymous data, and the new Data Protection Regulation" *Computer Law & Security Review* Volume 32, Issue 2 (2016) page 264 https://doi.org/10.1016/j.clsr.2015.12.013. Borgesius points out that although recitals do not hold the same legal value as provisions, they have interpretative value.

[26] Klimas and Vaiciukaite, "The law of recital in European Community legislation", page 92

mandate under the repealed Data Protection Directive, and functioned as *"an independent European advisory body on data protection and privacy"*.[27] The Working Party`s interpretations are

valuable to legal intepretations in the field of data protection law, although their opinions are not legally binding.[28] The Working Party does no longer exist, and the role it had has been taken over by the EDPB.[29] Like the Working Party, the EDPB is *"an independent European body, which contributes to the consistent application of data protection rules throughout the European Union…".*[30] It follows from Art 94 (2) GDPR that references made to the 29 Working Party *"…shall be construed as references to the European Data Protection Board established by this Regulation".*[31] I make several references to EDPB`s and the Working Party`s opinons and guidelines.

In my discussions I am conscious of the hierarchy that the different legal sources are placed in, in the sense that they carry different valuge/weight in a legal analysis. Even so, I have made extensive use of the EU Expert Bodies`opinions and guidelines, mainly the EDPB`s, despite these being "soft law". Through Art 70 GDPR the EDPB has been given a mandate to oversee that the regulation is applied in a correct and consistent manner.[32] This law-given role gives the EDPB gravitas and authority, and in my opinion legitimices the use of the EDPB`s opinons in a legal analysis such as this paper. EDPB is an expert body when it comes to interpreting the data protection law and the regulation, and will therefore be of value to the discussion, especially one where there is not much case law that directly addresses the question on the agenda.

I have researched case law from the European Court of Justice. I have not found many relevant judgements, and no judgements dealing with the specific discussion in this thesis, namely the principles in Art 5 (1)(a) GDPR in relation to manipulative marketing online.

---

[27] Article 29 Working Party Opinon 2/2010 on online behavioural advertising page 1

[28] Borgesius, "Singling out people without knowing their names – Behavioural targeting, pseudonymous data, and the new Data Protection Regulation", page 259

[29] Recital 139 in the GDPR preamble and Art 94 (2) GDPR. Also, in Art 68 (1) GDPR the European Data Protection Board is established, and according to Art 70 (1) GDPR *"The Board shall ensure the consistent application of this Regulation".*

[30] European Data Protection Board, "Who we are", access date 27 April 2022,
https://edpb.europa.eu/about-edpb/about-edpb/who-we-are_en

[31] Art 94 (2) GDPR

[32] Art 70 (1) GDPR and Art 70 (1)(a) GDPR

In some instances I make references to (or in relation with) the repealed Data Protection Directive, since the interpretations relating to the Directive are generally still relevant when disucsisng GDPR. The reasons for this argument: The GDPR replaced the directive,[33] and Art 94 (2) GDPR states that *"References to the repealed Directive shall be construed as references to this Regulation"*.

I have also found valuable source material in different legal articles, as well as some commentary from data protection authorities.

I want to comment on my methodology when discussing the lawfulness, fairness and transparency principles. In chapter 3 I have tried to give a structured discussion of the three principles, about their interpretation and application in regards to manipulative online marketing. I have divided the discussion into three sections, one for each principle. In each section I have a subsection where I view the selected examples of (potentially) manipulative practices in light of the principle. I have chosen to divide the principles into separate sections simply to give the discussion a clear structure, and hopefully give the reader a better overview. It is still important to view the principles together with one another, as they are closely connected. Some would even regard them as elements of one and the same principle.[34] This is supported by the fact that the principles are alle placed together in Art 5 (1) (a), as opposed to being separated into three different letters. On the other hand, they are dividied into three separate criterias/terms, instead of having just one term that contained all three elements. In addition to this, the recitals refer to them as principle*s*, plural, and not one single principle combined. For instance recital 60 refers to *"The principles of fair and transparent processing…"*.[35] I therefore argue that these are three separate principles, but with strong inter-connections/relations. Irrespective of them being viewed as separate principles or the same principle, the three terms (lawfulness, fairness and transparency) contain different elements that can be discussed separately.

[33] See Art 94 (1) GDPR where it is stated that the Data Protection Directive is repealed from the date that the GDPR entered into force.

[34] See Lee A. Bygrave *Data Privacy Law: An international Perspective* (Oxford: Oxford University Press 2014), Page 146, where Bygrave refers to the *principle* (singular) of fair and lawful processing.

[35] Recital 60 of the GDPR preamble

1.4 Thesis construction

In the introduction in section 1.1, I give context and background to the topic of discussion. In section 1.2 I explain the research question. In chapter 2 the term manipulation is first explained and discussed in a more general way, before it is discussed within the frames of GDPR and in connection with marketing, where I also connect the GDPR to the examples of manipulation practices that I have chosen to take a closer look at. Then, in chapter 3, comes the material discussion of the principles and how they can be used and viewed in relation with manipulative marketing, before some concluding remarks are made in chapter 4.

The thesis has a wide starting point, and is narrowed down by chapter 3. By starting wide and defining terms and laying the ground work in chapter 1 and 2, and then narrowing down the focus, the specific question I want to discuss and explore in chapter 3 can (hopefully) be understood in a more systemic and comprehensible way.

I have focused only on two explicit examples of manipulative online marketing, namely 1) third-party cookies, also called tracking cookies, and 2) targeted ads on social media platforms. These examples will be further explained in the following sections 2.2.3 and 2.2.4.

2 Manipulation and autonomy

2.1 Manipulation in general

Consumers are constantly being persuaded, bothered or even manipulated by advertisers. Companies pay big money to advertisers in order to create an ad that will hopefully catch the interest of their target group. Use of colors, slogans, placement of a product in a store; every aspect is thoughtfully construed in order to catch your eye. This is nothing new. What is relatively new however, is how advertisers now use the possibilities and tools that the digital world and the internet provide to gain more and more information about its prospective customers, in order to sell them products/services.

Before diving into a discussion about manipulative marketing, it is essential to clarify and determine the meaning of manipulation in the context of this paper. First of all, the term "manipulation" is not a term derived from GDPR. "Manipulation" is not mentioned in the GDPR at all. The definition of "manipulation" is based on articles/legal theory, but is also based on society`s common understanding of the word, and is not to be understood as merely a legal term. Although manipulation is not explicitly mentioned in the GDPR, there are terms and language in GDPR that is there to prevent manipulative processing. For instance fundamental principles in the GDPR such as lawfulness, fairness and transparency. More on this later on.

Shaun Spencer, in his article on online manipulation, refers to Susser et al and points out that Susser et al have defined manipulation as "*an intentional attempt to influence the subject that (1) is hidden from the subject, (2) attempts to exploit a subject`s "cognitive, emotional, or other decision-making vulnerabilities ", and (3) is "targeted" at those vulnerabilities"*.[36] Susser et al also suggests a simpler version of this definition, namely that manipulation is just any hidden influence.[37] Spencer proposes his own definition, namely that *"Manipulation is an intentional attempt to influence a subject's behavior by exploiting a bias or vulnerability."*[38] Spencer points

[36] Shaun B. Spencer, «The Problem with Online Manipulation» *University of Illinois Law Review* Vol 3 (2020) page 985-986
https://heinonline-org.ezproxy.uio.no/HOL/Page?handle=hein.journals/unilllr2020&id=973&collection=journals&index=

[37] Spencer, «The Problem with Online Manipulation», page 986

[38] Spencer, «The Problem with Online Manipulation», page 990

out that the defintions have in common an intent to influence, and that the influence is hidden from the subject.[39] It is the manipulative *mechanism* that needs to be hidden from the subject in order for there to be a manipulation, mechanism meaning the cognitive process that drives the subject to act in accordance with the manipulator`s wish, and not the manipulative stimulus/the "bait" if you will.[40] Spencer points out that manipulation must be distinguished from persuasion.[41] Regarding the criteria of intent: It makes sense that in order for there to be a manipulation, there has to be a degree of intention from the manipulator, meaning that the manipulation is intended to influence the subject in a certain way, it is not just a mere coincidence or something unintentional that occurs. However, it can be discussed how strong the intent has to be before there is a manipulative action. In my opinion, the threshold should not be very high before the criteria of intent is met. I would argue that also below this threshold there can be manipulation; if there is no intention but there is instead negligence/culpability. However, some might say that the core meaning of a manipulation is that it is a conscious, intentional act. I would argue in favour of a more open interpretation of the term manipulation, at least make an argument that there can be degrees to a manipulation, ranging from mild to severe.

Judith Vermeulen provides another description of what a manipulation is, and points out that "*A manipulator seeks to insinuate himself in a target's decision-making process and thus deprives the individual of the authorship over his or her ideas."*[42]

Vermeulen also argues that the practice of news personalisation can potentially be a threat to/and violation of freedom of thought and freedom to form opinions, if the degree of influence reaches an unacceptable level and amounts to interference.[43]

Vermeulen`s description of manipulation refers to the principle of autonomy. It points to the core aspect that where there is manipulation there is no autonomy ("authorship"). One of the

---

[39] Spencer, «The Problem with Online Manipulation», page 990

[40] Spencer, «The Problem with Online Manipulation», page 990

[41] Spencer, «The Problem with Online Manipulation», page 985

[42] Judith Vermeulen "Recommended for you: "You don`t need no thought control". An Analysis of News Personalisation in Light of Article 22 GDPR" in *Privacy and Identity Management. Data for better living: AI and Privacy*, editors Michael Friedewald, Melek Önen, Eva Lievens, Stephan Krenn and Samuel Fricker (Springer Nature Switzerland AG 2020, Switzerland: 2020) page 198

[43] Vermeulen "Recommended for you: "You don`t need no thought control". An Analysis of News Personalisation in Light of Article 22 GDPR", page 194

basic things about the concept of manipulation is that it takes away the individual`s autonomy/self-determination. Autonomy/self-determination is also an important part of privacy – and data protection law and the GDPR. Take for instance Art 8 in the European Convention on Human Rights, which stipulates the rigtht to respect for private life and family life.[44] In a judgement from the Euoprean Court of Human Rights, the Court stated that *"Article 8 of the Convention thus provides for the right to a form of informational self-determination, allowing individuals to rely on their right to privacy as regards data which, albeit neutral, are collected, processed and disseminated collectively and in such a form or manner that their Article 8 rights may be engaged."*[45] Within the GDPR we also see expressions of autonomy. Take for instance Art 25 GDPR about data protection by design and by default, which states that controllers shall design and execute processing in line with data subjects`rights and data protection principles, and implement appropriate measures in the design and operation to protect these rights.[46] As pointed out by the EDPB, an important aspect of data protection by design an default is autonomy, namely that *"Data subjects should be granted the highest degree of autonomy possible to determine the use made of their personal data, as well as autonomy over the scope and conditions of that use or processing."*[47] As EDPB points out, one objective of the GDPR is to give data subjects` more control over their personal data.

The concept of autonomy is also closely connected with the principles of fairness, lawfulness and transparency. Based on the definition of "manipulation" in this paper, autonomy is the antonym of manipulation. In order for individuals to have autonomy, the individuals have to be able to make informed decisions; they need information and transparency about any given process. Manipulation however, makes people take unconscious or unwilling decisions in accordance with the manipulator`s wishes. This can for instance happen through the use of technology where personal data is processed, which we will take a closer look at.

[44] Art 8 European Convention on Human Rights

[45] Case of Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland, Paragraph 137

[46] Art 25 (1) GDPR

[47] EDPB Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognise and avoid them page 10

2.1.1 Profiling/Online Behavioural Advertising (OBA)

Behavioural targeting, also referred to as online profiling, is about monitoring consumer`s online behavior in order to target them with individualized advertisments.[48] In the context of manipulation and online marketing it is highly relevant to discuss the concept of online behavioural advertising/ behavioural targeting, since the whole point of online behavioural advertising is to attempt to influence a consumer by knowing things about them, and then to utilize this information to target them with custom made advertisments.

This type of advertising has some core similiarities to what has been discussed about the term manipulation in section 2.1, in that the there is an intent behind the whole practice of influencing an individual in ways they are unaware of.

"Profiling" is defined in GDPR Art 4 (4) as *"any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;".*[49]

The Working Party has written an opinon about online behavioural advertising. In their opinion behavior advertising is defined as "*advertising that is based on the observation of the behaviour of individuals over time. Behavioural advertising seeks to study the characteristics of this behaviour through their actions (repeated site visits, interactions, keywords, online content production, etc.) in order to develop a specific profile and thus provide data subjects with advertisements tailored to match their inferred interests."*[50]

Online behavioural advertising raises serious privacy concerns. These concerns are so storng that the Norwegian Consumer Council, together with multiple other organizations and experts,

[48] Borgesius, "Singling out people without knowing their names – Behavioural targeting, pseudonymous data, and the new Data Protection Regulation", page 256

[49] GDPR Art 4 (4)

[50] Article 29 Data Protection Working Party Opinon 2/2010 on online behavioural advertising, page 4

have suggested a ban on what they call surveillance-based advertising.[51] This suggestion comes in the wake of their 2021 report "Time to ban surveillance-based advertising".[52] This type of advertising is also part of a larger problem that is surveillance capitalism as mentioned in section 1.1.

In section 2.2.3 and 2.2.4 I will explain the practices that I will focus on and use as examples of manipulation, namely third-party cookies (tracking cookies) and targeted ads derived from social media user data. These practices/technologies are both tools in the online behavioural advertising industry. Cookies for instance, are used to find out about consumer`s interests in order to target them with specific advertisments.[53] The techniques/practices that will be described in section 2.2.3 and 2.2.4, are part of the same system that makes online behavior advertising possible; utilizing large amounts of (personal) data for commercial gain. In what way these practices can be manipulative, and how the principles in Art 5 (1) a GDPR can protect against this manipulation, will be discussed in chapter 3.

Before diving into a discussion on the potentially manipulative nature of such practices, I will look more closely at the material scope of GDPR and manipulative practices within the scope of GDPR. This is explored in the following section.

2.2 Manipulation within the scope of GDPR

In the past section I discussed the term manipulation in a more general way, and how manipulation can be the result of online behavioural advertising. Now I will move onto the concept of manipulation within the scope of GDPR, and how GDPR can be relevant and applicable in this context.

---

[51] Forbrukerrådet (Norwegian Consumer Counsil) «International coalition calls for action against surveillance-based advertising", June 22 2021 https://www.forbrukerradet.no/side/new-report-details-threats-to-consumers-from-surveillance-based-advertising/

[52] Forbrukerrådet (Norwegian Consumer Council) "Time to ban surveillance-based advertising", June 2021 https://www.forbrukerradet.no/wp-content/uploads/2021/06/20210622-final-report-time-to-ban-surveillance-based-advertising.pdf

[53] Borgesius, "Singling out people without knowing their names – Behavioural targeting, pseudonymous data, and the new Data Protection Regulation", page 257

Galli writes about online behavoiur advertising and the issue of manipulation of data subjects/consumers, and notes that GDPR does not directly regulate either manipulative advertising or online behavior advertising, but that the GDPR can regulate online behavioural advertising indirectly whenever personal data is being processed, or when there is automated-decisions being made, with a reference to Art 22 GDPR.[54] Art 22 (1) GDPR states that *"the data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her"*.[55] Art 22 will not be further explored in this paper.

It follows from Art (5) (1) (a) GDPR that *"personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');"*[56] These principles are the basis for my discussion in chapter 3. Before discussing manipulative use of personal data for marketing purposes, and the legal protection these data protection principles give against such use, we first have to clarify the terms "personal data" and "processing" in the GDPR.

Art (2) section 1 GDPR states that "*the regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form a part of a filing system or are intended to form part of a filing system"*.[57] What section 1 states is that in order for GDPR to apply, the data concerned has to be 1) processed, the data being processed has to qualify as 2) "personal data", and the data has to be processed 3) wholly or partly by automated means.

2.2.1 Personal data

The first question is which types of data constitute personal data. In this thesis I will take a closer look at the data collected through third party cookies and social media platforms used for targeted advertisments qualify as personal data.

---

[54] Federico Galli, "Online Behavioural Advertising and Unfair Manipulation Between the GDPR and the UCPD" in *Algorithmic Governance and Governance of Algorithms*, editors Martin Ebers and Marta Cantero Gamito (Switzerland: Springer Nature Switzerland AG 2021, 2021) page 112-113

[55] Art 22(1) GDPR

[56] GDPR Art 5 (1) a

[57] GDPR Art 2 (1)

In Art 4 (1) GDPR, personal data is defined as *"any information relating to an identified or identifiable natural person ("data subject")"*. In the same section it is stated that *"an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as (...) an online identifier(...)"*. Other factors that relate specifically to an individual`s identity can also constitute information that can identify a specific person, such as information about physical appearances or their *"economic, cultural or social identity..."*.[58]

The mentioning of "an online identifier" is of particular interest. This term is further explained in recital 30 GDPR. Recital 30 states that: *"Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them."*[59] This means that if for instance a cookie identifier can be connected with a specific person, then that cookie identifier is defined as personal data. As is pointed out in recital 30, the use of cookies on user`s devices can potentially reveal their identity, in that case making it "personal data". The same goes for an IP-address, if this address can be connected with a specific person, which it often (but not always) can.

In the *Breyer* case from 2016, the European Court of Justice discussed the concept of personal data. The case regarded storing of dynamic IP-addresses, and if dynamic IP-addresses constituted "personal data".[60] The question was if Mr Breyer, who had used some governmental websites and had his IP-address collected and stored by the website provider, was identifiable through his IP-address.[61]

In paragraph 15 of the judgement, the ECJ explained what an IP address is:
"IP addresses are series of digits assigned to networked computers to facilitate their communication over the internet. When a website is accessed, the IP address of the computer seeking

[58] GDPR Art 4 (1)
[59] Recital 30 GDPR Preamble
[60] Case C-582/14 Breyer v Bundesrepublik Deutschland, Paragraph 31
[61] Case C-582/14 Breyer v Bundesrepublik Deutschland, Paragraph 24

access is communicated to the server on which the website consulted is stored. That connection is necessary so that the data accessed may be transferred to the correct recipient."[62]

Dynamic IP-addresses are defined as *"provisional addresses which are assigned for each internet connection and replaced when subsequent connections are made, and not 'static' IP addresses, which are invariable and allow continuous identification of the device connected to the network."*[63]

In paragraph 39 the court noted that *"…it must be ascertained whether such an IP address, registered by such a provider, may be treated as data relating to an 'identifiable natural person' where the additional data necessary in order to identify the user of a website that the services provider makes accessible to the public are held by that user's internet service provider."*[64] The court had to assess whether or not an IP-address, that in itself did not disclose the identity of a natural person/the person behind the IP-address, but that in connection with additional information held by the internet service provider, and not the website provider that had collected the IP-address, would make an indentification possible.

The issue was that the website provider had the IP-address but did not have access to the additional information that would connect the IP-address to Mr Breyer; that information was held by the internet service provider. But, as pointed out by the court in paragraph 43, *"(…)it is not required that all the information enabling the identification of the data subject must be in the hands of one person".*[65]

The court also noted that the identification can be both directly and indirectly, and pointed out that "*The use by the EU legislature of the word 'indirectly' suggests that, in order to treat information as personal data, it is not necessary that that information alone allows the data subject to be identified."*[66] This means that even though one piece of information is not enough in itself to identify a person, if you can combine the one piece of information with another piece

[62] Case C-582/14 Breyer v Bundesrepublik Deutschland, Paragraph 15
[63] Case C-582/14 Breyer v Bundesrepublik Deutschland, Paragraph 36
[64] Case C-582/14 Breyer v Bundesrepublik Deutschland, Paragraph 39
[65] Case C-582/14 Breyer v Bundesrepublik Deutschland, Paragraph 43
[66] Case C-582/14 Breyer v Bundesrepublik Deutschland, Paragraph 41

of information, and the two pieces combined would point to a specific person, then both pieces of information are considered personal data.

Recital 26 in the GDPR explains the above mentioned point in more detail:
"To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments".[67]

The ECJ concluded in the Breyer case that the dynamice IP-address that the online media service provider (the website provider) collected, did in fact constitute personal data, even though identification of the person behind the IP-address could only be revealed if the website provider also had access to additional information held by the internet service provider. Even though the website provider would not have such access unless they`d use legal steps (e.g. in the case of a cyber attack), this was still considered a *reasonable* (see reference to recital 26 GDPR above) means to use to identify the person.[68]

To sum up: An IP-address can be considered personal data according to the ECJ. Through this case we see that the term "personal data" is to be given a broad meaning, and that what constitutes personal data has a low threshold.

That the term "personal data" is to be given a wide meaning, was underlined by the Working Party in their opinon from 2007 on the concept of personal data.[69]

It is important to separate personal data from anonymous data. If the information is anonymous, it is not considered personal data: In recital 26 it is stated that the GDPR does not apply *"...to anonymous information, namely information which does not relate to an identified or*

[67] Recital 26 GDPR
[68] Case C-582/14 Breyer v Bundesrepublik Deutschland, Paragraph 47- 49
[69] Article 29 Data Protection Working Party Opinon 4/2007 on the concept of personal data page 4

identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable."[70] However, it is important to separate anonymous data from pseudonymous data, since the latter is still regarded as personal data: In recital 26 it is also pointed out that "*Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person".*[71] This means that even though the data in question is pseudonymous, it can still be viewed as personal data if it can be traced back to a natural person if additional data is applied.

Pseudonymous is a term that is also used within computer science language when talking about behavioural targeting, and refers to profiles of individuals that are built. These profiles are called pseudonymous, since the individual`s name is not evident just from this data.[72]

2.2.2 Processing

"Processing" is defined in Art 4 (2) GDPR "*as any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;"*[73] We see that collection and use of personal data, which is the focus in this paper, is covered by the definition.

This thesis is concerned with online marketing towards consumers and the data that is being processed from online users in this regard. For example, cookies that are placed on user`s computers in order to collect data; this is data "processing". This processing is also done through wholly or partly by automated means; it is not a human being collecting this data, these are machines/algorithms that have been programmed (by humans) to collect certain data.

---

[70] Recital 26 GDPR Preamble

[71] Recital 26 GDPR Preamble

[72] Borgesius, "Singling out people without knowing their names – Behavioural targeting, pseudonymous data, and the new Data Protection Regulation", page 258

[73] Art 4 (2) GDPR

The "manipulation" that this paper focuses on is manipulation of consumers through automatic processing of personal data. When advertisers have access to personal data, they (through the use of algorithms) can effectively place targeted ads, in ways we might not be fully aware of. It is about manipulation that involves using information about these customers/consumers to produce effects that these consumers are unaware of. Trick them in a way that they otherwise would not have wanted, had they been sufficiently informed.

The manipulative nature of the above mentioned practices/technologies, will not be discussed in the following sections, but in chapter 3.

2.2.3 Third-party cookies; what are they and do they process personal data?

When we are browsing the internet and visiting different webpages, different information about our browsing history is collected and stored. Use of cookies is one way of storing web browsing data. Cookies are defined as *"small text files that websites place on your device as you are browsing. They are processed and stored by your web browser."* [74] The information that is collected is for example *"(...)details of their IP address and other meaningful metadata(...)",*[75] which is then *"contained within instructions called HTTP headers and sent to the servers that are hosting the visited website."*[76] As was clarified in he Breyer case (see discussion above in section 2.2.1), IP-addresses are usually considered to be personal data.[77] The ECJ noted in the Breyer case that *"(...)in order to treat information as personal data, it is not necessary that that information alone allows the data subject to be identified."*[78] It is therefore safe to say that IP-addresses and cookie identifiers can often be considered personal data. I refer to the rest of my discussion in section 2.2.1 on the meaning of "personal data".

---

[74] GDPR.eu "Cookies, the GDPR, and the ePrivacy Directive" access date 29 March 2021 https://gdpr.eu/cookies/

[75] David Agogo "Invisible market for online personal data: An examination" *Electronic Markets* Vol. 31 Issue 4, 2021 Page 991 https://doi.org/10.1007/s12525-020-00437-0

[76] Agogo "Invisible market for online personal data: An examination", Page 991

[77] Case C-582/14 Breyer v Bundesrepublik Deutschland, Paragraph 47-49. See also Borgesius, "Singling out people without knowing their names – Behavioural targeting, pseudonymous data, and the new Data Protection Regulation", page 264, where the question whether or not IP-addresses constitute as personal data is discussed. The question is disputed by some, since the same IP-address can sometimes be used by many individuals, e.g university internet.

[78] Case C-582/14 Breyer v Bundesrepublik Deutschland, Paragraph 41

There are different types of cookies. Some cookies are essential in order for a webpage to function as intended and do not raise privacy concerns. There are however other types of cookies, typically third-party cookies, also called marketing cookies/tracking cookies, that raise privacy concerns.[79]

It is important to differentiate between first-party cookies and third-party cookies. First-party cookies are cookies that is placed on your device by the website you visit, as opposed to third-party cookies which are cookies placed on your device by third-parties and not the website you visit, for example an advertiser. Third-party cookeis can also be referred to as marketing cookies or tracking cookies, and is used to track your online activity, the data of which can be shared between different third-parties, such as advertisers.[80]

Third-party cookies can also take the form of a so-called social plug in, such as the Facebook "like" button, which is sometimes present at the front page of a website. Thic icon functions as a cookie and sends data to Facebook.[81]

The Working Party has argued that behavioural advertising that involves the use of tracking cookies, makes it possible for a specific computer to be singled out and is therefore to be regarded as personal data.[82]

Even if the data that the cookie stores does not directly identify the individual tied to this data, as long as it can indirectly identify the person behind the data, it is considered personal data. For instance if a website that uses cookies also requests your e-mail address, the data stored by the cookie can be connected to your e-mail address and identify you.[83] As is pointed out by Frederik Borgesius in his 2016 article on behavioural targeting; *"if a company processes nameless data about an individual, and it is fairly easy for another party to tie a name to the data, it*

---

[79] GDPR.eu "Cookies, the GDPR, and the ePrivacy Directive" access date 29 March 2021 https://gdpr.eu/cookies/

[80] GDPR.eu "Cookies, the GDPR, and the ePrivacy Directive" access date 29 March 2021 https://gdpr.eu/cookies/

[81] Case C-40/17 FashionID, Paragraph 25 and 27

[82] Article 29 Data Protection Working Party, Opinion 16/2011 on EASA/IAB Best Practice Recommendation on Online Behavioural Advertising page 8

[83] Borgesius, "Singling out people without knowing their names – Behavioural target-ing, pseudonymous data, and the new Data Protection Regulation", page 264

follows from the Data Protection Directive's preamble that the data are personal data."[84] Some argue that the data collected by cookies or other tracking used for behavioural advertising does not constitute as personal data, since they do not have a name or an address or other additional information that can point to a specific individual.[85] When it comes to data used for behavioural targeting, it is usually fairly easy for a company to connect the data to a name/an individual.[86] It can therefore be argued with some confidence that the data collected by cookies constitute personal data.

Tracking cookies have been much discussed in recent times because they are said to be declining and on their way out, a "decline" that has arguably been seen since around 2019, when the ECJ came with their judgement in the Planet 49 Case.[87] In Planet49 the ECJ ruled that where the user of a website consented to the use of third-party cookies by accepting an already pre-ticked checkbox stating the use of such cookies, was not in accordance with data protection law and the rules on lawful consent.[88] Some browsers have already phased out use of third-party cookies, and Google has announced that their browser Google Chrome will phase out the use of third-party cookies by 2023.[89] Google has made some suggestions as to what alternative technology could possibly replace the functions of third-party cookies in the context of behavioural advertising,[90] but nothing definite, so the future of tracking is not clear.

Even with these developments, it is in my opinion still relevant to discuss the practice of third-party cookies. This is due to the fact that third-party cookies are still very much in use, and until they are completely gone, they are relevant to discuss, even after they might be gone, if for no

---

[84] Borgesius, "Singling out people without knowing their names – Behavioural targeting, pseudonymous data, and the new Data Protection Regulation", page 265

[85] Tal Z. Zarsky "Privacy and Manipulation in the Digital Age", *Theoretical inquiries in law*, Volume 20 Issue 1 (2019) Page 167 https://doi-org.ezproxy.uio.no/10.1515/til-2019-0006

[86] Borgesius, "Singling out people without knowing their names – Behavioural targeting, pseudonymous data, and the new Data Protection Regulation", page 265

[87] Hubspot, "The Death of the Third-Party Cookie: What Marketers Need to Know About Google's 2022 Phase-Out" access data 10 May 2022 https://blog.hubspot.com/marketing/third-party-cookie-phase-out

[88] Case C-673/17, Bundesverband v Planet49, Paragraph 57

[89] Inc.com "Third-Party Cookies Are on Their Way Out. How to Prepare for What's Next" access date 10 May 2022 https://www.inc.com/magazine/202111/rebecca-deczynski/cookies-marketing-strategies-google-chrome.html, see also Google blogpost: Google, «Charting a course towards a more privacy-first web" access data 10 May 2022 https://blog.google/products/ads-commerce/a-more-privacy-first-web/

[90] Hubspot, "The Death of the Third-Party Cookie: What Marketers Need to Know About Google's 2022 Phase-Out" access data 10 May 2022 https://blog.hubspot.com/marketing/third-party-cookie-phase-out

other reason than for historical value. In addition to this, given the age of surveillance capitalism that we live in, we can proably claim with a degree of certainty that tracking practices will not go away, whether it be through use of tracking cookies or other technologies. As Zuboff writes in her book on surveillance capitalism*: "Right now we are at the beginning of a new arc that I have called information civilization, and it repeats the same dangerous arrogance. The aim now is not to dominate nature but rather human nature. The focus has shifted from machines that overcome the limits of bodies to machines that modify the behaviour of individuals, groups, and populations in the service of market objectives".* [91] Targeted advertisments and the techniques/technologies behind them is just a small part of this new economic order that Zuboff discusses in her book; surveillance capitalism. This is why I argue that the discussions in this paper regarding third-party cookies is relevant and valuable, regardless of the future of third-party cookies, since it is reasonable to expect tracking cookies to be replaced by another practice, with similar goals and functions with respect to tracking online user`s browsing history etc and capitalizing on this, which in turn raises similar privacy concerns.

2.2.4 Social media and targeted advertisments; processing of personal data?

In order to access and use an app/social media platform, the user has to accept the terms of use. Take for instance Instagram`s Data Policy. In section I of the policy, there is extensive information on which data the app collects, such as the data you provide when signing up to the app, data about the content you share and which accounts you visit, which Facebook groups you follow, IP-address and data from cookie identifiers on your device.[92] In section II of the data policy, there is information on how the data is used and for what purposes. There are many different uses and purposes, one purpose is serving the user with personalized advertisments.[93] We see that the social media platform collects a lot of personal data from its users, see section 2.2.1 regarding the definition of personal data.

---

[91] Zuboff, *The Age of Surveillance Capitalism – The fight for a human future at the new frontier of power,* page 515

[92] Instagram "Instagram Data Policy" Section I: What kinds of information de we collect?, Date of last revision 4 Jan 2022 https://help.instagram.com/519522125107875/?maybe_redirect_pol=0

[93] Instagram "Instagram Data Policy" Section II: How do we use this information?, Date of last revision 4 January 2022 https://help.instagram.com/519522125107875/?maybe_redirect_pol=0

The use of personal data to target social media users is something that has been discussed by the EDPB in their Guidelines 8/2020 on the targeting of social media users. Here they discuss the issue of how "*targeting sevices make it possible for natural or legal persons (''targeters'') to communicate specific messages to the users of social media in order to advance commercial, political or other interests''.*[94]

Targeting can be based on personal data collected either through data that is *provided* by the social media users (e.g. age in bio), or through *observed* data (e.g. the user`s activity on the social media platforms such as visited profiles, which content is liked/commented, but also the user`s activity outside the social media platform provided by a third-party actor). Targeting can also happen based on *inferred* data, which is predictions about the user`s assumed interests and/or needs that the targetor predicts based on the provided and/or the observed data.[95]

3 Principles in Art 5 (1) (a) GDPR and protection against manipulative online marketing

3.1 Introduction

Art 5 GDPR stipulates the basic principles governing processing under the GDPR.[96] The principles are important when interpreting the other provisions in the GDPR, but they are also enforceable, and violations of the principles can be sanctioned with heavy fines.[97] The primary principle of data privacy law is the principle of fair and lawful processing.[98] As Bygrave notes, this is the primary principle because *''it embraces and generates the other principles presented below''*.[99] Bygrave does not mention transparency alongside the criterias of fair and lawful, but

[94] EDPB Guidelines 8/2020 on the targeting of social media users Version 1.0 Page 3

[95] EDPB Guidelines 8/2020 on the targeting of social media users Version 1.0 Page 12-13

[96] Paul Voigt and Axel von dem Bussche *The EU General Data Protection Regulation* (Switzerland: Springer International Publishing 2017) Page 87. DOI 10.1007/978-3-319-57959-7

[97] See Art 83 (5)(a) GDPR. See also Voigt and von dem Bussche *The EU General Data Protection Regulation*, Page 87.

[98] Bygrave, *Data Privacy Law: An international Perspective*, Page 146

[99] Bygrave, *Data Privacy Law: An international Perspective*, Page 146. Some of the other principles that were presented: Minimality (page 151) and purpose limitation (page 153).

instead points out that within the fairness principle there is a criteria of transparent processing.[100] As I discussed in section 1.3, fairness, lawfulness and transparency can be regarded as three separate principles, or as criterias/elements part of the same principle.[101] In this paper they are viewed as three separate principles, but sharing strong connections.

I have chosen to only focus on the three principles in Art 5(1)(a) GDPR, and not the other principles in Art 5. Although I could also have discussed other fundamental principles in GDPR, I chose the mentioned principles, both because of the need to narrow down the discussion, but also because these are principles that are important contrasts/opposites to manipulation. In my opinon they touch the very core of what manipulation is *not*. Manipulation can be unlawful, unfair and non- transparent. These principles are also closely related to *consent* as a legal basis for processing personal data, which is a legal basis that is frequently used for the type of processing that is discussed in this paper, e.g processing through the use of third party cookies, which will be discussed in some detail later on.

The purpose limitation principle derveses to be mentioned, a principle which requires that personal data shall be *"collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes"*.[102] This principle is regarded by many experts as an especially important principle, and is particularly challenged in the context of big data analytics.[103] The purpose limitation principle is indirectly present within the principles of lawful, fair and transparent processing: In recital 39 of the GDPR preamble, where the closer content of the three principles is explained, it is noted that; *"(...)In particular, the specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data.*[104] With this said, the principle will not be discussed further here, because of the above mentioned reasons.

---

[100] Bygrave, *Data Privacy Law: An international Perspective*, Pages 146-147

[101] See Bygrave, *Data Privacy Law: An international Perspective*, Page 146, where Bygrave refers to the principle (singular) of fair and lawful processing. See recital 60 in GDPR preamble that begins with the wording "the principles of fair and transparent processing…". (principles, plural)

[102] Art 5(1)(b) GDPR

[103] Bygrave, *Data Privacy Law: An international Perspective*, Page 153

[104] Recital 39 GDPR Preamble

It is important to underline that Art 5 does not operate alone. The article has to be viewed together with other articles in the GDPR, and vice versa. For instance, Art 13 ("Information to be provided where personal data are collected from the data subject") and Art 14 ("Information to be provided where personal data have not been obtained from the data subject") are direct extensions/manifestations of the transparency principle.[105] It is however sufficient/valuable to discuss only Art 5 (1) (a) GDPR in relation with manipulative marketing, without having to discuss any other articles in the GDPR. This is due to the fact that any processing has to be in accordance with the principles in Art 5, regardless of its legality according to other articles in the GDPR. This was pointed out by the ECJ in the judgement Google v. Spain, where the ECJ noted that *"…all processing of personal data must comply, first, with the principles relating to data quality set out in Article 6 of the directive and, secondly, with one of the criteria for making data processing legitimate listed in Article 7 of the directive."*[106] The EDPB has also noted this, stating, the context being a discussion about consent as a legal bases for processing personal data, that *"(…)obtaining consent also does not negate or in any way diminish the controller's obligations to observe the principles of processing enshrined in the GDPR, especially Article 5 with regard to fairness, necessity and proportionality, as well as data quality. Even if the processing of personal data is based on consent of the data subject, this would not legitimize targeting which is disproportionate or unfair."*[107] Meaning, if a certain processing of personal data is in accordance with say for example Art 22, or Art 6, but is in violation of Art 5, the processing is illegal.

In the following section 3.2 I give an overview of the principles and look more closely at how the principles are connected. In section 3.3 I discuss the principle of lawfulness and to what extent it protects against manipulative marketing. In section 3.4 I will, in the same context, discuss the principle of fairness, and then the principle of transparency in section 3.5.

[105] Voigt and von dem Bussche, *The EU General Data Protection Regulation*, Page 88

[106] Case C-131/12 Google Spain Paragraph 71. Note: ECJ´s comment was made in relation with the now repealed Data Protection Directive, but the point still stands.

[107] EDPB Guidelines 8/2020 on the targeting of social media users Version 1.0 Page 16

3.2 Art 5 (1)(a) GDPR: The relevant principles in light of each other

According to Art 5 (1) (a) GDPR *"Personal data shall be (a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');".*[108]

It is clear that these principles are inter-connected, given that they are mentioned together under the same sub-section/letter.[109] The fairness and transparency principles are mentioned together in multiple recitals of the GDPR, namely recital 60 and 71.

In recital 60, it is stated that: *"The principles of fair and transparent processing require that the data subject be informed of the existence of the processing operation and its purposes. The controller should provide the data subject with any further information necessary to ensure fair and transparent processing taking into account the specific circumstances and context in which the personal data are processed. Furthermore, the data subject should be informed of the existence of profiling and the consequences of such profiling(...)."*[110]

In recital 60 you see how the two principles, fairness and transparency, are viewed in combination: For processing to be fair, it has to be transparent, and processing that is sufficiently transparent, is also likely to be fair.

In recital 39 all three principles are mentioned. In the first sentence it is stated that *"Any processing of personal data should be lawful and fair. It should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed."*[111]

---

[108] Art 5 (1) (a) GDPR

[109] See Gianclaudio Malgieri «The concept of fairness in the GDPR: A linguistic and contextual interpretation" article summary from a lecture held at the *FAT* '20: Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency* (2020) Page 155
https://doi-org.ezproxy.uio.no/10.1145/3351095.3372868

[110] Recital 60 GDPR Preamble

[111] Recital 39 GDPR Preamble

It is also worth noting that the articles in GDPR, including Art 5 (1) a, should be interpreted in the light of/in accordance with fundamental rights and freedoms. In Article 1 section 2 GDPR it is noted that "*This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.*"[112] The right to protection of personal data is also stipulated in Article 8 of the Charter of Fundamental Rights in the European Union (EU Charter). The EU Charter is explicitly mentioned in Recital 1 of the GDPR Preamble. The preamble also makes a reference to fundamental rights in several other recitals of the preamble.

It is important to view the principles in connection with each other. As I have now shown in some detail, they are inter-linked in multiple ways, and partially overlap. However, it is also important to view the principles separately, as they also have their own feet to stand on, which we will see in the following sections.

3.3 Lawfulness: How does the lawfulness principle protect against manipulative marketing online?

3.3.1 The lawfulness principle, third-party cookies and targeted ads on social media

The lawfulness principle is manifested through Art 6 GDPR titled "lawfulness of processing", where section 1 of the article lists 6 alternative legal grounds for processing personal data.[113] Section 1 letter a stipulates consent as one legal ground for processing, which is arguably the most relevant in the context of third-party cookies and data collected through social media used for targeted ads. Some of the issues relating to (the use of) consent and arguably the lack thereof is discussed in some detail on pages 36-37 under section 3.4.1 regardin the fairness principle. The same discussion is relevant when addressing the lawfulness principle, so I refer to the mentioned discussion.

[112] Art 1 (2) GDPR

[113] Elena Gil González and Paul de Hert "Understanding the legal provisions that allow processing and profiling of personal data—an analysis of GDPR provisions and principles" *ERA Forum* (2019) Page 599 https://doi.org/10.1007/s12027-018-0546-z

When discussing the lawfulness principle in relation with targeted ads based on data collected from social media, it is also interesting to take a look at Art 21 GDPR, and discuss whether or not this practice falls within the application of Art 21 GDPR. In section 1.2 I discussed the content and limitations of my research question. I also specified what I mean with the term "online marketing" and specified that the term is not mentioned in the GDPR. Art 21 GDPR does however, regulate data protection rights in relation with so-called "direct marketing". The close resemblance of the terms marketing and "direct marketing" begs the question if Art 21 is relevant when discussing manipulative online marketing, especially when discussing ads on social media that are targeted at the consumer/user.

According to Art 21 (2) GDPR the data subject has a right to object "*Where personal data are processed for direct marketing purposes(...)".*[114] Section 2 of the article further states that the right to objection also includes *"(...)profiling to the extent that is related to such direct marketing".*[115]

"Direct marketing" is not further explained or defined in GDPR, and we must therefore look elsewhere. The proposed ePrivacy Regulation Art 4 (3) litra f states that*""direct marketing communications" means any form of advertising, whether written or oral, sent to one or more identified or identifiable end-users of electronic communications services, including the use of automated calling and communication systems with or without human interaction, electronic mail, SMS, etc.;"*[116] It is important to underline that the ePrivacy Regulation is not yet enacted, so its value as a legal source is limited. However, it is natural to assume that the term as defined here, has the same meaning as in GDPR. The question is how to understand the wording "sent to one or more…" users, see the wording.

The Working Party has in their Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC) noted that the scope of the term "direct marketing" is "too limited".[117] The Working Party was concerned that the wording, especially the use of the word "sent", sets

[114] GDPR Art 21 (2)

[115] GDPR Art 21 (2)

[116] Art 4 (3) (f) Regulation on Privacy and Electronic Communications (proposal)

[117] Article 29 Data Protection Working Party Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC) page 20

a limiting criteria in that the marketing has to be sent/conveyed directly to an individual, which excludes most advertising online. They proposed that the article should be changed *"(...)to include all advertising sent, directed or presented to one or more identified or identifiable end-users. In addition, it should further be ensured that behavioural advertisements (based on the profiles of end-users) are also considered direct marketing communications directed at "one or more identified or identifiable end-users" (as such advertisements are targeted to specific, identifiable users)."*[118] As we see from this, the Working Party was arguing in favour of giving "direct marketing" a wider interpretation and application. With the wording being as it is now in the proposal, and without any clarification in the GDPR, it is probably difficult to argue that targeted ads on social media or on different websites online, are "sent" to the users, as it is more fitting to say that it is "presented to" or "directed at" the user, and not sent per se. The explicit examples of direct marketing which are mentioned in the definition given in the proposed ePrivacy Regulation, namely automated calling, electronic mail and text messages, further supports a more narrow interpretation of the term.

On the other hand, if you also focus on a theleological interpretation, then perhaps it can be argued that direct marketing also includes targeted ads that are personalized for specific users and then presented/directed at these users either on their social media platform or on websites they visit when browsing. The preamble does not say anything about the objective of Art 21, but a reasonable assumption is that the data subject is given this right to object because it is an intrusive way of marketing. The data subject is being singled out and contacted directly through channels such as e-mail. Although a social media account or browsing the internet is not of the same personal nature as e-mail or SMS, it certainly gives you a feeling of intrusion and surveillance when being presented with targeted ads on a regular basis. This is especially the case when you are on your social media platform, which is a place where you usually share aspects from your personal life with friends and family.

In a recent judgement from the ECJ, the issue of direct marketing under the ePrivacy Directive was discussed in relation with "inbox advertising", where the case concerned advertisments that

[118] Article 29 Data Protection Working Party Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC) page 21

resembled regular e-mails that were sent and displayed directly in the inbox.[119] Regarding the question of whether or not this qualified as direct marketing, the court noted that *"(...)it must be ascertained whether such a communication pursues a commercial purpose and is addressed directly and individually to a consumer."*[120] The Court confirmed that this was the case, and pointed to the nature of the advertising/message, namely that it was sent as a regular e-mail to a private inbox.[121] The Court did not use the opportunity to say anything more general about what might not quialify as direct marketing.

Given the uncertainty of how "direct marketing" is to be defined, and since it is arguably only applicable to more direct marketing such as marketing sent through e-mail or sms, I conclude that the term does not correspond with "online marketing" as it is used in this paper, and can not, in the context of this paper at least, be applied in relation with targeted ads on social media or targeted ads per se. It was still useful to clarify Art 21`s place in the discussion.

3.4 Fairness: How does the fairness principle protect against manipulative marketing online?

3.4.1 The fairness principle, third- party cookies and targeted ads on social media

As pointed out by Malgieri, the fairness principle is not mentioned alone in the GDPR, but always together with one or both of the two other principles.[122] Malgieri differentiates between transparent and fairly transparent. He points out that there is a difference, and that fairness adds something to transparency, namely that the data subject has *"(...)an actual knowledge of the data processing concerning him or her and of its main characteristics"*.[123] Malgieri points out that fair transparency is more than formal transparency, because fair transparency *"takes into account also "reasonable expactations" of data subjects*."[124] In this respect, it can be argued

[119] Case C-102/20 StWL Städtische Werke Lauf a.d. Pegnitz GmbH **v** eprimo GmbH, paragraph 20-21. See also the Court`s Press Release No 210/21, 25 November 2021 https://curia.europa.eu/jcms/upload/docs/application/pdf/2021-11/cp210210en.pdf

[120] Case C-102/20, paragraph 47

[121] Case C-102/20, paragraph 48

[122] Malgieri, «The concept of fairness in the GDPR: A linguistic and contextual interpretation", Page 156

[123] Malgieri, «The concept of fairness in the GDPR: A linguistic and contextual interpretation", Page 156

[124] Malgieri, «The concept of fairness in the GDPR: A linguistic and contextual interpretation", Page 157

that the fairness principle, compared with the other two principles up for discussion, brings a particular importance to the table, when discussing them in connection with manipulation, since the fairness principles is a form of qualitative transparency. Within the fairness principle also lies transparency that meets a certain standard. With this said, the three principles are important in themselves as well as together, and can be difficult to place on a "most valuable"- scale.

The EDPB defines the fairness principle as *"an overarching principle which requires that personal data should not be processed in a way that is unjustifiably detrimental, unlawfully discriminatory, unexpected or misleading to the data subject."*[125] Especially the last part of the definition is quite fitting in the context of this paper, given that manipulative processing of personal data is in fact misleading to the data subject.

The English Data Protection Authorities, specifically the Information Commisionor`s Office, has defined the fairness principles by dividing it into three parts: 1) transparency of the data processing, 2) effects on the data subject from the data processing and 3) the data subject`s expectations of the data processing.[126]

If we apply this 3-part model of the fairness principle on the concept of third-party cookies, it can be argued that the use of third-party cookies is in many instances not fair and not compliant with the fairness principle: 1) In many cases, the cookie banners declaring the use of cookies are not transparent, for instance in the way that the accept button is often much bigger and brighter than the reject button, the latter being often quite difficult to spot, or in some cases not there at all: See for instance www.xxl.no`s cookie banner:[127] The first time you visit their website, a cookie banner is shown. In the cookie banner there is a big green square with the words "Godta alle" (Norwegian for "accept all"), and in small text, blended in with the regular text with information about their use of cookies, at the bottom, it says "Avvis alle" (Norwegian for "reject all"). This is a good example of non-transparent communication. This practice of

[125] EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Version 2.0 Adopted on 20 October 2020, page 17-18

[126] Information Commissionor`s Office"Big data, artificial intelligence, machine learning and data protection" (2017) Pages 19-20 https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf, and Malgieri «The concept of fairness in the GDPR: A linguistic and contextual interpretation", Page 159

[127] https://www.xxl.no access date 30 April 2022. (The information is written in Norwegian since this is a Norwegian site.)

displaying links or other important information in a way that is easily overlooked, contrarty to the transparency principle, is a type of dark pattern that the EDPB calls "hidden in plain sight".[128] However, it should be noted that the website`s default setting is to only activate necessary cookies (first-party cookies, necessary for website functions), and not third-party cookies (marketing cookies/tracking cookies). The default setting are possible to see if you click on the "see details" box ("se detaljer" in Norwegian) next to "godkjenn alle". Here you see that only necessary cookies are activated/are on. This is an example of data protection by default. But, this is arguably an empty effort, as I imagine that many users will click on the green "accept all" button, since they might not even see the reject all option (I myself did not see the reject link at the first two-three glances at the textbox), and might not be bothered to "see details", which will result in the activation of all cookies they use, including tracking cookies/marketing cookies.

Another good example of non-transparent communication, and in my opinon much worse than the xxl.no-example above, is the cookie-banner that pops up on the website www.seher.no:[129] In this box there is no accept or reject option, only some very limited, arguably cryptic, information about their user policy, in addition to the two click-options ""Jeg forstår" (Norwegian for "I understand") or ""Les mer" (Norwegian for "Read more").
We can use Vermeulen`s definition of manipulation, by which it can be argued that the example above is an attempt "*…to insinuate himself in a target's decision-making process and thus deprives the individual of the authorship over his or her ideas."*[130]

2) The effects on the data subject is that the data subject`s browsing data/other data is being collected, possibly against the data subject`s wishes, and that the data subject is being presented with "relevant" ads throughout his/her web browsing session for X amount of time. On the other hand, some might think this is not invasive, and would not have a negative experience from it, but rather think it is practical or interesting to be presented with ads that possibly contain interesting offers. However, the point is that it should be completely the data subject`s own decision

[128] EDPB Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognise and avoid them page 19

[129] https://www.seher.no, access date 30 April 2022 (also a Norwegian site)

[130] Vermeulen, "Recommended for you: "You don`t need no thought control" ". An Analysis of News Personalisation in Light of Article 22 GDPR", page 198

whether or not to be "followed around" by ads, and by making it more difficult to reject such ads than to accept, this is not the case.

3) When it comes to the data subject`s expectations, it is to be assumed that most data subject`s would excpect to be informed in a clear and understandable way about how their data is being used. In other words they would expect transparency from the website provider.

Lack of fairness and transparency can also be found in the way that some of the biggest tech-companies use the data we provide through our online activitity, for instance Facebook and Google. As pointed out by Zuboff in her in depth analysis and discussion on surveillance capitalism, where e.g. the social media platform giant plays a central role, she explains the following: *"There have been myriad revelations of Google and Facebook`s manipulations of the information that we see. For now I´ll simply point out that Google`s algorithms, derived form surplus, select and order search results, and Facebook`s algorithms, derived from surplus, select and order the content of its News Feed."*[131] Zuboff talks about "surplus", or "behavioural surplus", which she defines as the exess data of our beahivoural data, meaning the data that is not used specifically for product or service improvement, but is exess, and is instead *"...fed into advanced manufacturing processes known as "machine intelligence", and fabricated into prediction products that anticipate what you will do now, soon, and later."* [132] The point she is making about how Facebook`s news feed works is that it uses the data we supply through our different activities on its platform to serve us with relevant or "meaningful" data.[133] Regarding how beavioural surplus data is being analyzed and used, Zuboff exemplifies by referring to a function that the Facebook algorithms at some point was revealed to have, where the function`s goal was *"to predict individuals who are "at risk" of shifting their brand allegiance. The idea is that these predictions can trigger advertisers to intervene promptly, targeting aggressive messages to stabilize loyalty and thus achieve guaranteed outcomes by altering the course of the future".*[134] The topics that Zuboff discusses are complex, as Zuboff is tackling an entire industry. These excerpts are only supposed to give a glimpse into the ways our digital footprints

---

[131] Zuboff, *The Age of Surveillance Capitalism – The fight for a human future at the new frontier of power*, page 185

[132] Zuboff, *The Age of Surveillance Capitalism – The fight for a human future at the new frontier of power*,page 8

[133] Zuboff, *The Age of Surveillance Capitalism – The fight for a human future at the new frontier of power*, pages 459-460

[134] Zuboff, *The Age of Surveillance Capitalism – The fight for a human future at the new frontier of power*, page 278

are being used in ways we do not understand, and very possibly do not like or approve of, had we known.

Regarding Facebook`s news feed and how its algorithms are designed, it has been revealed that the algorithms, which learn and indvidiualize your feed based on your activities/choices on the platform, at one point (note: my choice of word is because it is unclear from the source if the algorithms still operate in this way) was valuing angry emojis you gave to posts much higher than your "like" response. With such a setting it means that you are more likely to see content that makes you angry (hence the angry emoji you reply with) than content that makes you happy/content (hence the "like" response).[135]

Circling back to the meaning of the fairness principle; the fairness principle can aslo be sorted into two categories; procedural fairness and fair balancing. Fair balancing requires the processing to be proportional, meaning that different interests have to be weighed against necessity of processing purposes, while procedural fairness is more about the formal side of processing, e.g. transparency duties/measures.[136]

Another aspect of the principle is that it can be viewed in relation with the human right to respect for private life. GDPR makes several references to fundamental rights in its preamble, and protecting fundamental rights such as the right of protection of personal data is specifically mentioned in Art 1 section 2 GDPR as one of the regulation`s objectives. Art 8 (1) of the EU Charter also expresses that *"everyone has the right to protection of personal data concerning him or her".*[137] In Art 8 section 2 of the Charter we see a reference to the fairness principle, where it is noted that *"Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law".*[138] In this wording we also see an implicit reference to the lawfulness principle (I am referring to the part "…laid down by law"…). Art 8 (2) connects fairness with consent. The issue with consent can be seen as an issue connected with the fairness principle, given that the

[135] The Seattle Times, "How Facebook shapes your feed", last updated 27 October 2021 https://www.seattletimes.com/business/how-facebook-shapes-your-feed/

[136] Malgieri, «The concept of fairness in the GDPR: A linguistic and contextual interpretation", Page 157

[137] Charter of Fundamental Rights of the European Union Art 8 (1)

[138] Charter of Fundamental Rights of the European Union Art 8 (2)

fairness principle sets demands as to how information is given. Gonzalez and Hurt discuss the fairness principle in connection with consent, and in this context points out that *"...where a company provides information about its terms of service in a way that is difficult to understand, consent has not been obtained in accordance with the GDPR".*[139] This part of the principle is highly relevant when it comes to the practice of third party cookies and how they are used and presented by website providers. There are obviuously variations in how they are presented, but in many instances the cookie declaration and consent-form is not user-friendly. I refer to the examples mentioned above, where the design of these cookie-banners are problematic if the legal basis for this processing is consent, which is likely. Art 4 (11) GDPR defines consent as "freely given…".[140] Without going into further detail, it can be argued quite strongly that consent in the examples mentioned above would not be freely given.

Much of companies`data processing is based on a notice and consent system, which has been criticized for its shortcomings in that the notices are often long and difficult to understand.[141] In a notice and consent system, presentation is everything. The consumer wants to access a website, but is immediately met with a cookie banner, which probably is felt as a nuisance. This makes it even more important to make rejecting just as easy as accepting cookies, which is often not the case. Even if the information is given in a way that is transparent, there is still the question whether or not the consumer is bothered with or even competent to actually make an active choice, instead of just clicking on whatever is fastest and easiest. As pointed out by Nouwens et al, people are prone to prefer short-term benefits over long-term privacy.[142] These observations have led to the view of notice and consent systems as being merely "illusory in practice".[143] This begs the question (not to be answered in this paper) if a notice and consent system is actually counter-productive and damaging, and perhaps lacking *fair* transparency.

---

[139] Elena Gil González and Paul de Hert "Understanding the legal provisions that allow processing and profiling of personal data—an analysis of GDPR provisions and principles" *ERA Forum* (2019) Page 616 https://doi.org/10.1007/s12027-018-0546-z

[140] Art 4 (11) GDPR

[141] Miads Nouwens et al "Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence" *Proceedings of the 2020 CHI Conference on human factors in computing systems* (2020) Page 2-3 https://doi-org.ezproxy.uio.no/10.1145/3313831.3376321

[142] Nouwens et al, "Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence", Page 3

[143] Nouwens et al, "Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence", Page 3

In the context of the practice of consent, I want to note that Nouwens et al points to a specific development in the US, where some senators have suggested a prohibition, instead of operating with notices and concent. These senators have introduces a draft bill that suggests "(…)*that it should be prohibited for any large online operator to "design, modify, or manipulate a user interface with the purpose or substantial effect of obscuring, subverting, or impairing user autonomy, decision-making, or choice to obtain consent or user data."*[144] It would be interesting to discuss the prospect of having a prohibition system instead of leaving it up to the consumer to decide. With this said, this is a discussion of its own and will not be explored in this paper.

3.5 Transparency: How does the transparency principle protect against manipulative marketing online?

3.5.1 The transparency principle, third-party cookies and targeted ads on social media

The transparency principle is closely connected with the fairness principle.[145] This is also evident from the previous discussion of the fairness principle. When it comes to the closer content of the transparency principle, the recitals in the GDPR offers some guidance: In GDPR Recital 39 it is stated that *"(...)The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used(...)".*[146] Here we see that transparency is all about *how* information is presented to the data subject. Again we see strong parallels to the the fairness principle, see section 3.4.

The transparency principle set forth in Art 5 (1)(a) is also the basis for some of the articles in the GDPR, particularly Art 12 (Titled "Transparent information, communication and modalities for the exercise of the rights of the data subject"), Art 13 (Titled "Information to be provided

[144] Nouwens et al, "Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence", Page 3

[145] EDPB Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognise and avoid them, page 23

[146] GDPR Recital 39

where personal data are collected from the data subject") and Art 14 (Titled "Information to be provided where personal data have not been obtained from the data subject"). Art 12 (1) reiterates some of the wording in the above mentioned recital 30, and states that *"The controller shall take appropriate measures to provide any information(...)relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language(...)."*[147] Art 13 is also interesting, as it requires that the controller(s) gives the data subject certain categories of information in relation with the processing, such as that the controller informs about the *"the purposes of the processing for which the personal data are intended as well as the legal basis for the processing".*[148] Here we see the close ties with other fundamental principles such as the lawfulness principle, and also the purpose limitation principle set forth in Art 5(1)(b) GDPR.

Regarding the meaning of the transparency principle in relation with advertising, the EDPB has noted the following: *"The EDPB recalls that the mere use of the word "advertising" would not be enough to inform the users that their activity is being monitored for the purpose of targeted advertising. It should be made transparent to individuals what types of processing activities are carried out and what this means for the data subject in practice. Data subjects should be informed in an easily understandable language if a profile will be built based on their online behaviour on the platform or on the targeter's website, respectively, by the social platform and by the targeter, providing information to the users on the types of personal data collected to build such profiles and ultimately allow targeting and behavioural advertising by targeters. Users should be provided with the relevant information directly on the screen, interactively and, where appropriate or necessary, through layered notices."*[149]

Based on the guidelines from EDPB, the transparency principle entails many requirements with respect to what information the data subject should receive and in what manner. E.g., as the EDPB states, the user *"should be provided with the relevant information directly on the screen, interactively and, where appropriate or necessary, through layered notices"*.[150] Based on my personal experience when using social media platforms and when browsing the internet, this is not the current standard.

---

[147] Art 12 (1) GDPR

[148] Art 13 (1) (c) GDPR

[149] EDPB Guidelines 8/2020 on the targeting of social media users Version 1.0 Page 25, Section 84

[150] EDPB Guidelines 8/2020 on the targeting of social media users Version 1.0 Page 25, Section 84

One point of discussion is the transparency within the app when it is being used, another point of discussion is the transparency when signing up, particularly the terms of agreement/user policy that the user has to consent to in order to access the platform. As pointed out in section 2.2.4, Instagram`s data policy does inform about what type of data is collected and how the data is used in the form of layered notices (as required according to the EDPB, see above), which makes it more accessable and understandable.[151] However, there is a big volume of information, and as is noted by Laux et al in their article on online behavioural advertising; *"...even if the Terms and Conditions of digital platforms mention the use of OBA and similar methods, it cannot be assumed that consumers are actually reading them, let alone understand their implications."*[152] Especially the last part of the quote is important; even if a user reads through all of the information in the notice, it is in my opinion often difficult to get a good understanding of how the processing actually works in practice. This part of the discussion is regarding the quality of transparency, and we have therefore moved into the area of the fairness principle and fair transparency (see discussion on this in section 3.4).

The way data policies are often shaped and formulated today, it can be argued that they are not fully in accordance with either the transparency or perhaps especially the fairness principle. For instance, when terms of use etc are divided into sections/layered, depending on the layout, it might turn into a dark pattern that the EDPB calls "privacy maze".[153] This is where the information is given in layers and divided into sections, which can initially be a good way to make big volumes of information more accessible, but it can become so layered to the point where the reader/user loses oversight and does not get a structured overall view of the terms.[154] This dark pattern can in my opinon be detected when reading a user agreement such as Instagram`s or Facebook`s. Although the layering is giving the information a good structure, it can get

[151] Instagram "Instagram Data Policy", Date of last revision 4 January 2022 https://help.instagram.com/519522125107875/?maybe_redirect_pol=0

[152] Johann Laux, Sandra Wachter and Brent Mittelstadt «Neutralizing online behavioural advertising: Algorithmic targeting with market power as an unfair commercial practice" *Common Market Law Review* Volume 58 Issue 3 (2021) Page 729 https://kluwerlawonline-com.ezproxy.uio.no/JournalArticle/Common+Market+Law+Review/58.3/COLA2021048

[153] EDPB Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognise and avoid them page 26

[154] EDPB Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognise and avoid them page 26

overwhelming because there are so many sections and hyperlinks and dividing of information, to the point where users may lose oversight.

The issue mentioned above, where the user gets lost in all the information, resembles another dark pattern which the EDPB calls "too many options". This pattern referrs to a situation where the data subject/user wants to alter the data protection settings, but is finding this difficult because in order to do this the user has to go through many different pages, finding information in different locations and/or going through a multitude of options. This makes it potentially challenging for the user to be able to make the desired alterations in the settings, and can therefore be in breach of the transparency and/or fairness principle.[155]

As was discussed in chapter 2, a manipulator can be defined as someone that *"...seeks to insinuate himself in a target's decision-making process and thus deprives the individual of the authorship over his or her ideas."*[156] The question is if this definition can be applied to targeted advertisments on social media platforms. The EDPB points to the risk that targeting could lead to/amount to manipulation of social media users.[157] The EDPB gives an example of such manipulation, namely that an analysis of a user`s data could say something about the user`s emotional state, for instance through his/her use of hasthtags/keywords, which could then be used to target the user at a specific time when they are presumably more receptive to a specific product/message.[158] What if a user is posting about insecurities such as a having a bad body image, could they then potentially be targeted with ads for make-up or other body products? Based on the points given by the EDPB, it might seem like this could be the case, or at least something similar to this. Algorithms analyzing a user`s emotional state in order to target them can arguably lead to a more severe form of manipulation. Less intrusive ways for user data to be used in ways that could still be seen as borderline manipulative, could for instance be specific ads targeting young people/children, who are presumably more easily influenced than older people, e.g. ads for cosmetic products and/or treatments, such as fillers, eyelashextensions, self-tan creams, weight pills, etc.

---

[155] EDPB Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognise and avoid them page 40

[156] Vermeulen, "Recommended for you: "You don`t need no thought control". An Analysis of News Personalisation in Light of Article 22 GDPR", page 198

[157] EDPB Guidelines 8/2020 on the targeting of social media users Verison 1.0 Page 5

[158] EDPB Guidelines 8/2020 on the targeting of social media users Version 1.0 Page 6

As pointed out by Judith Vermeulen, the practice of news personalisation can potentially be a threat to and violation of freedom of thought and freedom to form opinions, if the degree of influence reaches an unacceptable level and amounts to interference.[159] Vermeulen`s fear is well-founded. To move beyond advertising; as is seen for instance on Facebook, personalized and filtered news creates ecco-chambers, where you are shown news that correspond with/enhances a specific view/standpoint you have, instead of being shown news that diversifies and nuances this very view/standpoint.

The same concern goes for personalized marketing: When a consumer is presented with ads for products/services that they might not have thought about at all, it can create false needs. Especially if a certain type of ad is shown multiple times. Predictions about which ads might interest a specific user are made based on a user`s activities on the platform and on other sites.[160] These predictions might cause other negative effects, for instance pressure or insecurity for the data subject. Take for instance a woman around 30 years old using Instagram. If she is viewing content of people with babies, the algorithms will register this, and she is likely to be presented with advertisments regarding babies/baby products. Seeing such ads/content on a regular basis can possibly contribute to increased pressure for the woman to start thinking about having babies, pressure that otherwise might not be felt so strongly.

We see that online marketing can be manipulative in the way that it is being personalized and targeted at specific consumers. In section 3.3 the transparency principle was explained, so how can the principle be applied to this type of manipulation? How is this type of manipulation deviating from the standards that the transparency principle sets? For starters, we see that the practice of using personal data to create targeted advertisments is quite covert. We know that these predictions are made by complex algorithms, but it is not clear for the consumer how this process actually works in detail. In this context is also worth mentioning Art 22 GDPR. Art 22 (1) GDPR states that "*The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal*

[159] Vermeulen, "Recommended for you: "You don`t need no thought control". An Analysis of News Personalisation in Light of Article 22 GDPR", page 194

[160] Facebook.com ,"How does Instagram decide which ads to show me?", access date 10 May 2022 https://www.facebook.com/help/instagram/173081309564229

effects concerning him or her or similarly significantly affects him or her."[161] Targeted advertising/ online behavioural advertising is mostly the result of a fully automated process.[162] This makes it relevant to also mention Art 22 GDPR in this context. It would be interesting to discuss the legality of manipulative marketing in the context of Art 22 GDPR, as is done by Galli in his article from 2021.[163] However, this falls outside the scope of the discussion in this thesis.

3.5.1.1 Design of cookie banners

When discussing the transparency principle, one highly relevant aspect to discuss is the design of cookie banners. This was discussed in some detail in section 3.4 regarding the fairness principle, but is also relevant here.

In a 2019 experiment on cookie banner design, the architecture of cookie-banners were alternated in order to see the difference in accept-rates depending on the layout of the banner: The experimenters alternated between a banner that made it just as easy to reject cookies as accepting them, and another banner where the accept button was much more available and appealing than the reject button. The website visitors had to go through multiple steps in order to get to the rejection-options. The experiment showed that many more visitors accepted cookies when the architecture of the banner made the reject-button harder to find, as opposed to the architecture where the reject-button was equally available as the accept-button. The results strongly supported the claim that having a specific architecture of the cookie-banner would "nudge" the visitor into accepting cookies.[164]

Privacy activist Max Schrems` organization NOYB ("None of your business"), has developed a program that identifies illegal cookie banners online. In 2021 they filed multiple complaints

---

[161] Art 22 (1) GDPR

[162] Forbrukerrådet (Norwegianl Consumer Counsil) «Time to ban surveillance-based advertising", Page 8, June 2021 https://www.forbrukerradet.no/wp-content/uploads/2021/06/20210622-final-report-time-to-ban-surveillance-based-advertising.pdf

[163] See Galli, "Online Behavioural Advertising and Unfair Manipulation Between the GDPR and the UCPD", pages 117 - 121

[164] Jan M. Bauer, Regitze Bergstrøm, Rune Foss-Madsen, «Are you sure, you want a cookie? – The effects of choice architecture on user`s decisions about sharing private online data" *Computers in Human Behavior 120* (2021) pages 2-4. DOI: https://doi.org/10.1016/j.chb.2021.106729

with different data protection authorities (DPAs) against companies who use(d) cookies illegally.[165]

Aanother example of questionable design of cookie banners on websites is the cookie banner on the Norwegian website of Foodora, which is explained in detail in the following:

Example: www.foodora.no:

When you visit Foodora`s webpage, a cookie banner comes up. In the banner there is a big pink button labelled "aksepter alle" (Norwegian for "accept all") and two much more neutral buttons (not pink), one labelled "Mer informasjon" (Norwegian for "more information") and one labelled "Lagre innstillinger (Norwegian for "Save settings"). If you click the accept all-button, all cookies are activated, including the marketing cookies, as opposed to only the essential cookies if you click on "save settings" without doing any changes. If you click on the "more information" box, two "menus" comes up side by side. Menu 1 is called "categories" (In Norwegian: "kategorier") and menu 2 is called "services" (In Norwegian: "Tjenester"). Below these menus is a "save settings"-button. In menu 1 about categories, you see that there are three categories of cookies that they use; marketing, functional and essential cookies. Only essential cookies are activated (and not possible to deactivate). When you click on "services", a list of the different cookies comes up, and below each is a small description stating what category the cookie belongs to. One marketing cookie is called "Facebook Pixel". When you click on it a whole submenu of different descriptions about it comes up, everything from a description of the function of the cookie to the legal basis for the cookie (which is Art 6 (1) (a) GDPR; consent). There is also information on the storage period, which is maximum 720 days. There is also information about what type of data that is collected, and for this specific cookie the list is extra long; for instance geographic location, IP-address, visited sites, device- ID and which ads and what content the user clicks on.[166]

This is definitely among the relatively "better" designed cookie banners, but it is in my opinion still a good example of a cookie banner that does not have a transparent enough way of

[165] noyb.eu, "noyb files 422 formal GDPR complaints on nerve-wrecking "Cookie Banners" " 10 August 2021, https://noyb.eu/en/noyb-files-422-formal-gdpr-complaints-nerve-wrecking-cookie-banners

[166] foodora.no, access date 10 May 2022 https://www.foodora.no/

presenting the data subject`s options in terms of which cookies to allow. It is also concerning to see how much data the marketing cookies collect about our online activities.

4 Conclusion

In this paper I have discussed the lawfulness principle, fairness principle and transparency principle, and discussed how they are important when faced with manipulation in the online marketing sphere. The principles are tightly connected and overlap in some ways.[167] Yet they are different and have individual value (see discussion in section 3.3-3.5). As a methodical choice, I consistently used the two same examples of manipulative tendencies in online marketing when discussing the different principles, these examples being 1) third-party cookies/tracking cookies used to create targeted advertisments and 2) the collection and use of personal data from social media users in order to create targeted advertisments. By discussing these two practices, I argued how manipulation can occur, and how these practices can at times be in violation of one or more of the three principles.

Although a few additional paragraphs in the GDPR were mentioned, we see that the principles are enough to be discussed on their own, given that the principles must be respected, regardless of whether or not other provisions in the regulation are complied with.[168] I have also argued that the principles in Art 5 (1) (a) are particularly relevant when discussing manipulative practices, since the very core of the principles` meaning are the opposite of what manipulation is. Take for example the fairness principle, which contains a requirement that data processing is not misleading to the data subject.[169] Of the three principles, although they all have individual (and combined) value and importance, based on the discusisons in this paper I lean towards the fairness principle having slightly more importance, at least in some aspects when discussing protection against manipulative online marketing. The EDPB calls it an "*overarching principle which requires that personal data should not be processed in a way that is unjustifiably detri-*

[167] Malgieri, «The concept of fairness in the GDPR: A linguistic and contextual interpretation", Page 155

[168] EDPB Guidelines 8/2020 on the targeting of social media users Version 1.0, Page 16

[169] EDPB Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognise and avoid them page 8

mental, unlawfully discriminatory, unexpected or misleading to the data subject.".[170] Fairness also contains within it a requirement of transparency; fair transparency.[171] Meaning you can`t have fairness without also having transparency that meets a certain standard.

When the term manipulation was discussed in chapter 2, we saw that there are different defintions, but that manipulation at its base is about the lack of autonomy.[172] I have also discussed a specific type of manipulation, namely dark patterns, and referred to some examples of dark patterns, e.g. "hidden in plain sight" or "privacy maze", see sections 3.4.1 and 3.5.1 respectively. There are several types of dark patterns,[173] and only some have been pointed out in this paper. Still, this paper offers a view into our digital reality, where the main take away is probably the overwhelming amount of information and the complexity of the information that is sprung on us, which leaves us often feeling helpless. There is however protection to be found in the discussed principles, and we see that they are at times not complied with. In some instances it can be argued on both sides as to whether or not the principles discussed in this paper are complied with, as they are not clear cut in their definitions, this can for instance be said of some user agreements`that are structured/layered but also long and confusing, see section 3.5.1 (pages 40-41). However, for some examples that we have seen in this paper, it can be argued strongly that there is manipulation in place, and hence non compliance with the principles, e.g. manipulative layouts of certain cookie banners, see section 3.4.1 (page 34).

[170] EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Version 2.0 Adopted on 20 October 2020, page 17-18

[171] Malgieri, «The concept of fairness in the GDPR: A linguistic and contextual interpretation", Page 156

[172] Vermeulen, "Recommended for you: "You don`t need no thought control". An Analysis of News Personalisation in Light of Article 22 GDPR", page 198. See also EDPB Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognise and avoid them, page 10 (Autonomy is explained to be an important objective of privacy by design and by default)

[173] See EDPB Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognise and avoid them

Table of reference

Legislation:

General Data Protection Regulation	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 945/46/EC
EU Charter	Charter of Fundamental Rights of the European Union (2012/C 326/02)
ECHR	European Convention on Human Rights Rome, 4 November 1950
ePrivacy Directive	Directive 2002/58/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic commu- nications sector (Directive on privacy and electronic communications)
Unfair Commercial Practices Directive	DIRECTIVE 2005/29/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Di-rective 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council

European Court of Justice (ECJ) judgements

ECLI:EU:C:2016:779	Case C-582/14 Breyer v Bundesrepublik Deutschland
ECLI:EU:C:2014:317	Case C-131/12 Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González
ECLI:EU:C:2019:801	Case C-673/17 Bundesverband der Verbraucherzentralen und Verbraucherverbände — Verbraucherzentrale Bundesverband eV v Planet49 GmbH
ECLI:EU:C:2019:629	Case C-40/17 Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV
ECLI:EU:C:2021:954	Case C-102/20 StWL Städtische Werke Lauf a.d. Pegnitz GmbH v eprimo GmbH

European Court of Human Rigths judgements

Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland	The European Court of Human Rights Strasbourg, 27 June 2017

European Data Protection Board (EDPB), guidelines and opinions

Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Version 2.0, adopted on 20 October 2020

Guidelines 8/2020 on the targeting of social media users, Version 1.0, adopted on 2 September 2020

Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognise and avoid them, Version 1.0, adopted on 14 March 2022

European Data Protection Supervisor (EDPS), guidelines and opinions

Opinion 3/2018 on online manipulation and personal data, adopted on 19 March 2018

Article 29 Data Protection Working Party (Working Party), guidelines and opinions

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

Opinion 4/2007 on the concept of personal data (01248/07/EN WP 136), adopted on 20 June 2007

Opinion 16/2011 on EASA/IAB Best Practice Recommendation on Online Behavioural Advertising (02005/11/EN WP 188), adopted on 8 December 2011

Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC), adopted on 4 April 2017

Other soft law:

Proposal for a ePrivacy Regulation:	COM (2017) 10: Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communi-cations and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)

Proposal for Digital Services Act	Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC

Articles with DOI:

Elena Gil González and Paul de Hert "Understanding the legal provisions that allow processing and profiling of personal data—an analysis of GDPR provisions and principles" ERA Forum (2019) 19: Pages 597–621
DOI: https://doi.org/10.1007/s12027-018-0546-z

Nouwens, Miads et al. "Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence" *Proceedings of the 2020 CHI Conference on human factors in computing systems* (2020) pages 1-13
DOI: https://doi-org.ezproxy.uio.no/10.1145/3313831.3376321

Yeung, Karen "Hypernudge: Big Data as a mode of regulation by design" *Information, Communication & Society* 20:1 (2017) pages 118-136.
DOI: 10.1080/1369118X.2016.1186713

Ball, Kirstie and William Webster «Big Data and surveillance: Hype, commercial logics and new intimate spheres" *Big Data & Society* Volume 7 Issue 1 (2020) Pages 1-5
DOI: https://doi.org/10.1177%2F2053951720925853

Bauer, Jan M., Bergstrøm, Regitze and Foss-Madsen, Rune. «Are you sure, you want a cookie? – The effects of choice architecture on user`s decisions about sharing private online data" *Computers in human behavior* 120 (2021) pages 1-7
DOI: https://doi.org/10.1016/j.chb.2021.106729

Agogo, David "Invisible market for online personal data: An examination" *Electronic Markets* Vol. 31 Issue 4, 2021 Page 989 – 1010
DOI: https://doi.org/10.1007/s12525-020-00437-0

Zuiderveen Borgesius, Frederik J., "Singling out people without knowing their names – Behaioural targeting, pseudonymous data, and the new Data Protection Regulation"
Computer Law & Security Review Volume 32, Issue 2 (2016) pages 256 - 271
DOI: https://doi.org/10.1016/j.clsr.2015.12.013

Zarsky, Tal Z. "Privacy and Manipulation in the Digital Age", *Theoretical inquiries in law,* Volume 20 Issue 1 (2019) pages 157-188
DOI: https://doi-org.ezproxy.uio.no/10.1515/til-2019-0006

Malgieri, Gianclaudio «The concept of fairness in the GDPR: A linguistic and contextual interpretation" in *FAT* '20: Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency* (2020) Pages 154–166
https://doi-org.ezproxy.uio.no/10.1145/3351095.3372868

Articles without DOI:

Spencer Shaun B. «The Problem with Online Manipulation» *University of Illinois Law Review* Vol 3 (2020) pages 959-1006
https://heinonline-org.ezproxy.uio.no/HOL/Page?handle=hein.journals/unilllr2020&id=973&collection=journals&index=

Laux, Johann, Wachter, Sandra and Mittelstadt, Brent, «Neutralizing online behavioural advertising: Algorithmic targeting with market power as an unfair commercial practice" *Common Market Law Review* Volume 58 Issue 3 (2021) Pages 719–750 https://kluwerlawonline-com.ezproxy.uio.no/JournalArticle/Common+Market+Law+Review/58.3/COLA2021048

Klimas, Tadas ; Vaiciukaite, Jurate "The law of recital in European Community legislation" *ILSA journal of international & comparative law*, Vol 15 Issue 1 (2008), pages 63-93 https://heinonline-org.ezproxy.uio.no/HOL/Page?lname=&public=false&collection=journals&handle=hein.journals/ilsaic15&men_hide=false&men_tab=toc&kind=&page=63#

Forbrukerrådet (The Norwegian Consumer Counsil) Report "Out of control – How consumers are ex-ploited by the online advertising industry" (2020)
https://fil.forbrukerradet.no/wp-content/uploads/2020/01/2020-01-14-out-of-control-final-version.pdf

Forbrukerrådet (The Norwegian Consumer Council) Report, "Time to ban surveillance-based advertising" (2021)
https://www.forbrukerradet.no/wp-content/uploads/2021/06/20210622-final-report-time-to-ban-surveillance-based-advertising.pdf

Forbrukerrådet (Norwegian Consumer Counsil), Report "Deceived by design: How tech companies use dark patterns to discourage us from exercising our rights to privacy» (2018) https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf

Information Commissionor`s Office, "Big data, artificial intelligence, machine learning and data protection" (2017) https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf

Chapter in books

Vermeulen, Judith. "Recommended for you: "You don`t need no thought control". An Analysis of News Per-sonalisation in Light of Article 22 GDPR". In *Privacy and Identity Management. Data for better living: AI and Privacy*, edited by Michael Friedewald, Melek Önen, Eva Lievens, Stephan Krenn and Samuel Fricker. Pages 190- 205. Switzerland: Springer Nature Switzerland AG 2020, 2020

Galli, Federico. "Online Behavioural Advertising and Unfair Manipulation Between the GDPR and the UCPD". In *Algorithmic Governance and Governance of Algorithms*, edited by Martin Ebers and Marta Cantero Gamito. Pages 109-135. Switzerland: Springer Nature Switzerland AG 2021, 2021

Books

Zuboff, Shoshana. *The Age of Surveillance Capitalism – The fight for a human future at the new frontier of power.* USA: Profile Books, 2019.

Voigt, Paul, and von dem Bussche, Axel. *The EU General Data Protection Regulation*. Switzerland: Springer International Publishing, 2017.
DOI 10.1007/978-3-319-57959-7

Bygrave, Lee A. *Data Privacy Law: An international Perspective*. Oxford: Oxford University Press 2014.

Web pages

European Data Protection Board, "Who we are", Access date 27 April 2022,

https://edpb.europa.eu/about-edpb/about-edpb/who-we-are_en

The Economist “How Apple`s privacy push cost Meta $10 bn”, Publication date 3 February 2022 https://www.economist.com/the-economist-explains/2022/02/03/how-apples-privacy-push-cost-meta-10bn

Forbrukerrådet (Norwegian Consumer Counsil) «International coalition calls for action against surveillance-based advertising”, Publication date 22 June 2021 https://www.forbrukerradet.no/side/new-report-details-threats-to-consumers-from-surveillance-based-advertising/

Collins dictionary “Definition of targeting”, access date 4 March 2022 https://www.collinsdictionary.com/dictionary/english/targeting

The Seattle Times, “How Facebook shapes your feed”, last updated 27 October 2021 https://www.seattletimes.com/business/how-facebook-shapes-your-feed/

Instagram, “Instagram Data Policy” Date of last revision 4 January 2022 https://help.instagram.com/519522125107875/?maybe_redirect_pol=0

Google, «Charting a course towards a more privacy-first web” access data 10 May 2022 https://blog.google/products/ads-commerce/a-more-privacy-first-web/

Inc.com “Third-Party Cookies Are on Their Way Out. How to Prepare for What's Next”, access date 10 May 2022 https://www.inc.com/magazine/202111/rebecca-deczynski/cookies-marketing-strategies-google-chrome.html

Hubspot, “The Death of the Third-Party Cookie: What Marketers Need to Know About Google's 2022 Phase-Out”, access date 10 May 2022 https://blog.hubspot.com/marketing/third-party-cookie-phase-out

Facebook.com, “How does Instagram decide which ads to show me?”, access date 10 May 2022 https://www.facebook.com/help/instagram/173081309564229

noyb.eu, “noyb files 422 formal GDPR complaints on nerve-wrecking “Cookie Banners” ” Publication date 10 August 2021, https://noyb.eu/en/noyb-files-422-formal-gdpr-complaints-nerve-wrecking-cookie-banners

foodora.no, access date 10 May 2022 https://www.foodora.no/

gdpr.eu, “Cookies, the GDPR, and the ePrivacy Directive” access date 11 May 2022 https://gdpr.eu/cookies/

XXL.no, (front page), access date 30 April 2022 https://www.xxl.no

Seher.no, (front page), access date 30 April 2022 https://www.seher.no

Court of Justice of the European Union Press Release No 210/21, Luxembourg 25 November 2021 https://curia.europa.eu/jcms/upload/docs/application/pdf/2021-11/cp210210en.pdf