



universität
wien

MASTERARBEIT / MASTER'S THESIS

Titel der Masterarbeit / Title of the Master's Thesis

„Unmasking the platform economy under the Digital
Service Act: a critical analysis of digital risks posed to
society“

verfasst von / submitted by

Nivine El-Aawar

angestrebter akademischer Grad / in partial fulfilment of the requirements for the degree of
Master of Arts (MA)

Wien, 2024 / Vienna 2024

Studienkennzahl lt. Studienblatt /
degree programme code as it appears on
the student record sheet:

UA 066 589

Studienrichtung lt. Studienblatt /
degree programme as it appears on
the student record sheet:

Masterstudium Internationale Entwicklung

Betreut von / Supervisor:

Univ.-Prof. Dr. Michaela Pfadenhauer

Abstract (English)

The new emerging platform economy has been accompanied by transformation processes within the economy, society and politics. In the course of this, platform businesses have become powerful actors, which are posing risks to society and democracy. This has become evident during recent events, such as the spread of misinformation during the Covid-19 pandemic, voter manipulation through social media or disinformation campaigns in ongoing wars. In view of this, the calls for regulations increased to which the European Union reacted by adopting the “Digital Service Act” (DSA) in 2022. This can be described as the first attempt to regulate platform businesses on an international level. The regulation is grounded on a risk-based approach, that imposes due diligence obligations on Very Large Online Platforms (VLOPs) and assigns private businesses the role of digital risk regulators. Considering the economic logic of platforms, it is unclear how digital risks are linked to the data-driven businesses models and what implications this has for the DSA. That is why this thesis critically examined VLOPs by illustrating how the digital risks outlined in the DSA are deeply interwoven with the process of monetising (personal) data. The case study analysis of TikTok and Instagram revealed that the digital risks of misinformation/disinformation, negative effects on mental/physical wellbeing, negative effects on children/young adults and discrimination/bias are linked to the business models of the platforms. Particularly the technology employed, such as the algorithmic recommendation system and automated content moderation, have been shown to generate and reinforce digital risks, as they are mainly employed for profit-oriented purposes irrespective of the effects on society and individuals. In that sense, this thesis concludes that digital risks may represent an essential component of the platform economy because some of the systematic risks identified by the DSA are deeply intertwined with the way profit is generated by VLOPs. That is why the EU should not shift the responsibility of regulating digital risks towards private businesses, to prevent the regulation from becoming a “toothless tiger”.

Abstract (Deutsch)

*Die Plattformökonomie wird von Transformationsprozessen in der Wirtschaft, Gesellschaft und Politik begleitet. Im Zuge dessen, entwickelten sich Plattformunternehmen zu mächtigen Akteuren, welches mit Risiken für die Gesellschaft und die Demokratie einhergeht. Dies haben jüngste Ereignisse, wie die Verbreitung von Fehlinformationen während der Covid-19-Pandemie, Wähler*innenmanipulation durch soziale Medien oder Desinformationskampagnen in aktuellen Kriegen, gezeigt. Vor diesem Hintergrund wurden die Rufe nach Regulierung lauter, worauf die Europäische Union mit der Verabschiedung des "Digital Service Act" (DSA) im Jahr 2022 reagierte. Der DSA kann als erster Versuch betrachtet werden,*

Plattformunternehmen auf internationaler Ebene zu regulieren. Die Verordnung fußt auf einem risikobasierten Ansatz, der „sehr großen Online-Plattformen“ (Very Large Online Platforms) Sorgfaltspflichten auferlegt und privaten Unternehmen die Rolle von Risikoregulatoren für die Gesellschaft zuweist. In Anbetracht der wirtschaftlichen Logik von Plattformunternehmen ist unklar, wie digitale Risiken mit den datenbasierten Geschäftsmodellen verknüpft sind und welche Auswirkungen dies auf die Umsetzung des DSA hat. Daher wurden in der vorliegenden Arbeit Plattformunternehmen kritisch untersucht, indem aufgezeigt wurde, dass die, im DSA identifizierten, digitalen Risiken eng mit dem Monetisierungsprozess von personenbezogenen Daten verwoben sind. In diesem Zusammenhang ergab die Fallstudienanalyse von TikTok und Instagram, dass die digitalen Risiken der Fehlinformation/Desinformation, der negativen Auswirkungen auf das psychische/physische Wohlbefinden, der negativen Auswirkungen auf Kinder/junge Erwachsene und der Diskriminierung/Bias eng mit den Geschäftsmodellen zusammenhängen. Es konnte gezeigt werden, dass insbesondere die eingesetzten Technologien, wie das algorithmische Empfehlungssystem und die automatisierte Inhaltsmoderation, digitale Risiken erzeugen und verstärken, weil sie hauptsächlich zu gewinnorientierten Zwecken eingesetzt werden, ungeachtet der Auswirkungen auf die Gesellschaft und Individuen. In diesem Sinne kommt diese Arbeit zu dem Schluss, dass digitale Risiken einen essenziellen Bestandteil der Plattformökonomie darstellen, da einige der von dem DSA ermittelten systematischen Risiken eng mit der Art und Weise verwoben sind, wie Plattformunternehmen Gewinne erwirtschaften. Aus diesem Grund sollte die EU die Verantwortung für die Regulierung digitaler Risiken nicht auf private Unternehmen verlagern, um zu verhindern, dass die Regulierung zu einem "zahnlosen Tiger" wird.

Table of Contents

List of Figures and Tables	III
List of Abbreviations	III
1. Introduction.....	1
2. The Digital Risk Society	4
2.1 Theoretical background	5
2.1.1 The Risk Society	5
2.1.2 Overview of risk definitions.....	8
2.2 The Digital Risk Society.....	12
2.2.1 Overview of digital risk definitions	12
2.2.2 Characterising the Digital Risk Society	15
3. The Platform Economy	19
3.1 Introducing the platform economy	19
3.2 Overview of platform definitions	21
3.3 Value in the platform economy: the drive for data	25
4. The Digital Service Act.....	31
4.1 Towards a Digital Service Act	33
4.2 The Digital Service Act	35
4.2.1 Scope and scale of application	35
4.2.2 Due diligence obligations.....	37
4.2.3 Mitigation Measures.....	45
4.2.4 Liability	46
5. Methodology	48
6. Case Study Analysis: Digital risks as a side effect of social media businesses?	56
6.1 Characterising social media.....	56
6.1.1 Overview of social media definitions.....	56
6.1.2 TikTok	58
6.1.3 Instagram.....	59
6.1.4 The economic logic of TikTok and Instagram.....	60
6.2 Digital risks and social media.....	69
6.2.1 Misinformation and Disinformation.....	69
6.2.2 Physical and Mental Wellbeing	78
6.2.3 Children and Young Adults	82
6.2.4 Discrimination and Bias	85
6.3 Digital risks and the platform economy	89

7.	Discussion: Platforms as the new digital risk evaluators in the Digital Risk Society?.....	97
8.	Conclusion	102
9.	References.....	III

List of Figures and Tables

Figure 1 Providers covered by the DSA	36
Figure 2 TikTok For You Page	65
Figure 3 Instagram Feed	65
Figure 4 Misinformation on Instagram	76
Figure 5 Content restriction on Instagram	84
Figure 6 Meta subscription	90
Table 1 Due diligence obligations in the Digital Service Act.....	37

List of Abbreviations

DSA – Digital Service Act
VLOPs – Very Large Online Platforms
EU – European Union
DMA – Digital Markets Act
VLOSEs – Very Large Online Search Engines

1. Introduction

Platform businesses have become increasingly relevant to public and private life, which is accompanied by transformation processes within the economy, society and politics (Poell, Nieborg, & van Dijck, 2019, p. 1). In the early years, digital platforms were linked to perspectives of progress, which were thought to facilitate democracy through technological innovations (Heldt, 2022, p. 69). Those perspectives have increasingly been challenged due to recent developments (Rodríguez de las Heras Ballell, 2021, pp. 75–76).

The rapid changing and flexible nature of platforms has enabled them to operate in a sphere which became very profitable and was little regulated. This enabled the platform businesses to set their own rules and take advantage of the new emerging platform economy. In view of this, new digital markets were created, which mainly focus on monetising (personal) data (Schneider, 2018, p. 131). This has posed risks to society and democracy, which has become evident during events and scandals in recent years. Particularly the voter manipulation through social media in the context of the US-elections in 2016 or the UK Brexit campaign, hate speech against refugees in Germany, disinformation campaigns during elections and the spread of misinformation during the Covid-19 pandemic have affected the discourse around digital platforms (Heldt, 2022, p. 70). This is particularly important from the perspective of International Development Studies, as the outlined developments and digital risks immensely affect areas related to the academic field, such as radicalisation, racism, discrimination (class, gender, race) and colonialism. That is why it is crucial to have a look at digital risks and the developments from an International Development perspective, as many of the global processes are driven by businesses from the Global North, which have crucial effects on society, politics and economics (Poell et al., 2019, p. 2).

Given this, concerns have been raised regarding the transparency and accountability of online platforms (Kalbhenn, 2021, p. 49). Since the governments and International Institutions could not keep up with the rapid transformations linked to emerging platform economy and the increasing threats arising from this, the calls for regulations became louder. The European Union reacted to the calls by adopting the “Digital Service Act” (DSA) in 2022 as part of their digital strategy “Shaping Europe’s digital future”, which should encourage trustworthy technology, foster a democratic society, enable a sustainable economy, help to fight climate change and enable a green transition (European Commission, 2020b).

The Digital Service Act represents the first international regulation, which acknowledges that platform businesses pose risks to society. The DSA focuses on reinforces the responsibility and

accountability of private businesses, through imposing due diligence obligations on them, which should protect society and individuals. In that regard the DSA has identified systematic risks, which are stemming from Very Large Online Platforms (VLOPs) and factors that may influence the systematic risks, such as the algorithmic recommendation system or automated content moderation. The regulation is grounded on a risk-based approach, which obligates VLOPs to conduct a risk assessment and develop mitigation measures for the digital risks stemming from their services (see European Union, 2022).

Particularly social media platform are linked to digital risks arising from their services, as they have become an essential part of individuals' daily lives. A report for the European Union has highlighted that over 70 % of EU citizens use social media platforms daily (Gawer & Srnicek, 2021, p. 19). Social media platforms can be characterised as data-driven business models, which have become relevant players in the platform economy (Srnicek, 2017, pp. 254–255). Their business model is based on generating, extracting and analysing personal data by using technologies, which enables them to predict valuable human behaviour and interests for profit (Breidbach & Maglio, 2020, p. 164; Huhtala, 2019, p. 56; Siegel, 2013; Trzaskowski, 2022, p. 449; Zuboff, 2019, pp. 65–66). That is why this thesis focuses on social media platforms, as their monetisation process of personal data is representative of the general practices of platforms.

The DSA shifts the governmental responsibility of protecting society towards the private businesses (Gregorio & Dunn, 2022, pp. 2–3). In the light of the economic logic of platforms it is unclear to what extent the systematic risks identified in the DSA stemming from the VLOPs are linked to their business models. This raises the question if private businesses can and should be actors, which take up the role of digital risk regulators for society. Therefore, it is relevant to understand the key mechanisms of the platforms and what effect this has on society to be able to democratically regulate digital risks (Poell et al., 2019, p. 9). That is why this thesis is concerned with the following research question:

How are digital risks, which arise from social media platforms linked to the data driven value creation within the platform economy? And what are the implications in the context of the Digital Service Act?

To be able to answer the research question firstly digital risks and the digital risk society will be conceptualised by drawing from the traditional work around risks and the risk society by scholars such as Ulrich Beck (1992 (first 1986)) and Anthony Giddens (1999). The research around risks and the risk society will be extended by the limited but current research on digital

risks and the digital risk society. Providing an overview of the state of the art will enable to develop an understanding of what digital risks are and what implications they have for society.

This will be followed by an introduction to the platform economy, which focuses on defining platforms and giving insights into the data-driven value creation of platform businesses. In that regard platforms will be characterised, by highlighting their business practices and technologies used for monetising data. Due to the use of the social media platforms “TikTok” and “Instagram” as case studies the focus will be set on the monetisation of personal data, as it is particularly relevant in the context of digital risks and the research question.

The Digital Service Act is then outlined, by first showing why the DSA was adopted by the EU in the first place and secondly outlining the content of the regulation. The due diligence obligations for Very Large Online Platforms will be described, which are grounded on a risk-based approach. In view of this, the identified systematic risks, potential factors that may influence the risks and mitigation measures will be examined in detail.

Considering this the thesis integrates perspectives from: (1) a sociological (2) an economic (3) a legal pillar. Those three pillars will be combined in a case study analysis of digital risks, which will be explained in the methodology of this thesis.

In the light of the research question the platforms TikTok and Instagram will be used as illustrative examples. First, social media platforms are characterised as business models of the platform economy, which will be followed by the introduction of TikTok and Instagram, highlighting that they can be characterised as data-driven business models of the platform economy. A specific focus will be set on how the platform businesses function and what technology they employ to generate profit. This will be linked back to the data-driven value creation of the platform economy.

In a second step studies are outlined which have researched digital risks on TikTok and Instagram. Due to the large scope of digital risks, the focus will be on the following chosen digital risks outlined in the DSA: (1) misinformation/ disinformation (2) mental/physical wellbeing (3) children/ young adults and (4) discrimination and bias.

The purpose of the case study analysis is to answer the research question by showing that digital risks may represent a prerequisite for the platform economy because some of the systematic risks identified by the DSA are deeply intertwined with the way VLOPs generate profit. That is why the results from the digital risk analysis will be linked back to the economic logic of platform businesses.

Finally, the results will be discussed in the context of the DSA, questioning the role, which the EU has assigned to the private businesses as digital risk regulators for society.

2. The Digital Risk Society

In academic research, little attention has been paid to investigating social theories of risk society in the context of current technological developments (Sundberg, 2023, p. 1). Calls for revising the “digital risk society” have been made, but little research has been done in the past 15 years (Grenz, 2023, p. 105). That is why for this thesis only a very limited amount of current academic literature regarding the digital risk society could be found. Nevertheless, the research currently emerging around the digital risk society appears to be reasoned by its relevance to recent developments around digital risks. Particularly in the context of governmental regulations around technology, risk-based approaches have moved to the centre of attention. Thence the intersection of risks, technology and society needs investigation (Gregorio & Dunn, 2022, pp. 2–3). Therefore, it is crucial to revisit the theoretical work linked to the digital risk society, forming a new analytical perspective on current developments and regulations around digital risks.

Social theories of risk society are striking in this context, because they underline, that technology has become uncoupled from social control (Ekberg, 2007, p. 346). Hence, using the digital risk society as an analytical framework enables an understanding of current developments and debates around digital risk (Lupton, 2016, p. 301). Particularly in the context of governmental regulations, such as the Digital Service Act, it is important to understand where the academic debates around risks and society originated from and where the current developments can be positioned.

Social theories that focus on risks originated from a critique of approaches that measure risks mainly in numbers and characterise risks as objective facts (Ekberg, 2007, p. 350). Sundberg (2023) has identified two literature streams in which he positions the digital risk society. First, the work of Ulrich Beck (1992 (first 1986), 2008) and Anthony Giddens (1999) on the risk society and second, academic work on “how technological development is deeply linked to social development” (Sundberg, 2023, p. 2). This identification and positioning will be followed, due to the influence and importance of the work from the authors mentioned for the debates around risks and society. Despite the importance of the traditional work on the risk society, only the relevant aspects will be outlined for this thesis, noticing that the complex theoretical debates around the risk society cannot be fully covered. The focus will be on what

role technology plays within the traditional concepts around the risk society, which allows contextualising the current research and debates around the digital risk society.

This is especially the case for the work of Ulrich Beck, which is often referred to by current researches on an international level, as his work was deeply influential in debates around risks and society (see Grenz, 2023; Lupton, 2016, 2023; Sundberg, 2023). Due to the limitations of this thesis, his work will only be outlined by focusing on his latest work on digital risks. Choosing the latest work as a starting point is of particular importance because many of the arguments that have been made in earlier works such as *The Risk Society* (1992 (first 1986)) have been revised, changed and extended (Rasborg, 2018, p. 167). Based on his latest work “the Metamorphosis of the World” (2017), only relevant aspects from his older work are used in this thesis, underlining that his complex theory and debates around it cannot be explained to the fullest.

2.1 Theoretical background

2.1.1 The Risk Society

As a first step, a short introduction to “*The Risk Society*” (1992 (first 1986)) will be given, as this book was deeply influential for international debates around risks and his later work. The book was first published in 1986 in Germany, during a time in which a deep fear in the public regarding technological and natural disasters was present. Various events in the 80s such as the nuclear disaster in Chernobyl, forest dieback, debates around nuclear power, chemical accidents, etc. caused that fear. This background information is important to keep in mind, as the early work of Beck can be characterised as a product of the *Zeitgeist* (Jarvis, 2007, pp. 23–24; Rosa, Renn, & McCright, 2015, pp. 33–35).

In his book “*Risk society: towards a new modernity*” (1992 (first 1986)) Beck claimed that society has transformed from an industrial era towards a risk society (Sundberg, 2023, p. 3). Recognising, that all societies have been subject to risks, the concept of “risk society” focuses on the contemporary era (Lupton, 2023, p. 71). Beck underlines with his modernisation theory that a paradigm shift can be identified, which goes along with the new emerging risk society (Beck, 1992 (first 1986), pp. 19–20). That is why he proposes a new social theory underlining that previous social theories are linear theories and thus theories of reproduction fail to understand new emerging developments and changes (Knöbl, 2017, p. 5).

The so-called “first age of modernisation” was linked to “optimism and linear progress”, which scientific knowledge was a driver for and which was enforced by national states (Sundberg,

2023, p. 3). Influence on nature and society based on science and technology was linked to progress that increased wealth. In the so-called “second modernity”, this changed due to the negative side effects of the scientific and technological developments (Curran, 2013, p. 47). That is why in the modern era new risks occurred, which were characterised by their global nature, incalculability and lack of accountability (Rosa et al., 2015, p. 73). Against this background traditional institutions, such as the state started losing stability (Knöbl, 2017, p. 3). That was the case because institutions were responsible for driving the progress in the first age of modernisation, which is why they became questionable in the second modernity, as risks to society started to result from the developments (Sundberg, 2023, p. 3).

The theory of risk society critically examines the “rational nature” of science and technology (Ekberg, 2007, p. 345). Hence, in the second modernity, a shift from the focus on natural risks towards technological risks can be identified (Sundberg, 2023, p. 3). Beck concludes that systematic side effects of modernisation result in produced risks that play a crucial role in how modern society is structured (Curran, 2013, p. 47).

That is why in the risk society a conflict between the *goods* and the *bads* arises (Jong, 2022, p. 1). The goods refer to things such as wealth, labour or social security. The bads explain the external side effects of the means with which the goods were created (Beck, 2017, p. 93). The centrality of the production of goods becomes less relevant, due to the growing production of risks (Curran, 2013, p. 46). The distribution of bads (risks) becomes the centre of the risk society, rather than the distribution of the goods, which was characteristic for the first modernity (Jong, 2022, p. 1). This is linked to one of the main assumptions of Beck, that all individuals are being threatened by risks, independent from traditional categories that structure society, such as class or geographical boundaries (Rosa et al., 2015, p. 70). This modern individualisation process highlights, that the individual is at the centre of the structures of modernity (Jong, 2022, p. 1). Against that background, Beck underlines traditional categories cannot understand modern social structures but rather have to be understood through the lens of risk production (Beck, 1992 (first 1986), pp. 39–40).

In summary, the risk society is constituted based on three aspects (1) the transformed relationship of risk, time and space (2) the changed nature of risks and (3) the failure of institutional systems of insurance (Mythen, 2021, pp. 535–536).

Risks in modern society are revealed through “reflexive modernity”, meaning that a reflection process is taking place, focusing on uncertainties caused by modernisation (Sundberg, 2023, p. 3). The concept of reflexive modernity is the foundation of the risk society. It describes an

increased awareness of living in a society filled with unpredictable risks arising from modern science and technology (Ekberg, 2007, p. 345). This recognition of the limits of modern knowledge is characteristic of the meaning of reflexive modernity (Rosa et al., 2015, p. 79). In the following, only a short outline of the concept will be given, which does not provide a complete description, due to its complex nature. The shift towards reflexivity is a side effect of modernisation and describes a form of “applying the principles of modernisation” through confrontation, examination and critique (Lupton, 2023, p. 74). Given this reflexive modernity is a nuanced concept. Following Beck (1992 (first 1986)) reflexive modernisation characterises the unintended consequences of knowledge, which lead to reflexivity, which describes “a critical evaluation of the recognition of the limits to our knowledge” (Rosa et al., 2015, p. 79). Reflexivity in this context means a form of “self-confrontation” as an unintended side effect of the modern. Reflexive modernisation can lead to a “creative (self)- destruction of the industrial society” (Lupton, 2023, p. 74). As Giddens (1999) puts it reflexive modernity is linked to understanding the limits and contradictions of the modern on the one side, whilst on the other side enabling a reflection process, that opens up possibilities and an expansion of choice and engagement (Giddens, 1999, pp. 5–6).

Deeply influenced by events such as the world financial crisis of 2007/8 and the threat of global terror networks, Beck extends his theory to the “world risk society” (2008), which underlines the global nature of modern risks calling for a cosmopolitan formation of theory (Rosa et al., 2015, p. 74). The development from the risk society towards a world risks society marks a cosmopolitan turn in Becks' theory (Rasborg, 2018, p. 160). The focus of the world risk society lies on risks that are manufactured and not external risks, which poses questions regarding the causes of global risks in the world risk society (Jong, 2022, p. 6).

The world risk society is characterised by three main types of risks (1) environmental (2) financial and (3) terrorism risks (Rasborg, 2018, p. 161). This illustrates the development of Beck's social theory. In his early work, the focus was on unintended risks, such as natural disasters, which were extended by intended consequences, such as terrorism (Rosa et al., 2015, p. 72). Beck moves from his perception of a risk society being a “catastrophe society” towards the world risk society being a society in which global risks are “anticipated”. Concluding, that cosmopolitical solutions are needed due to risks not being bound to borders (Rasborg, 2018, p. 161).

In that regard, it is important to mention that the works of Beck have been heavily criticised (Knöbl, 2017, p. 7). In the following, only a few aspects of the criticism will be pointed out due to the limitations of this thesis.

Most importantly Beck was particularly criticised for his approach towards risks. The “totalisation” of risks and putting risks at the centre of modern society, neglects other factors structuring modern society, such as class relations¹ (Curran, 2016, pp. 42–43). Particularly the aspect, that the risk society is characterised by risks that affect individuals in an egalitarian way, leading to class structures being replaced by risk structures must be seen critically and questioned (Curran, 2013, p. 45).

Moreover, the risk society fails to give attention to how risks are experienced in countries of the Global South (Lupton, 2023, p. 90). The concept of the risk society has been criticised as being “Western-centric”, due to the insufficient acknowledgement of how risks are distributed unequally in the global context (Mythen, 2021, p. 538).

Another popular criticism concerns the argument that society has entered a new era (Knöbl, 2017, p. 7). The argument, that due to the different qualitative roles of risks in the modern a new epoch was entered lacks evidence (Curran, 2016, pp. 42–43). In the context of digitalisation, this argument is interesting, because it is questionable to what extent the current technological developments lead into a new era and have a revolutionary potential (Egard & Hansson, 2023, p. 763).

The criticism mentioned leaves the question open if the theory of risk society is suitable to analyse current developments and modern risks (Curran, 2016, p. 42). Whether or not modern society has entered a new epoch is left unanswered, but it can be concluded that modern risks, particularly in the context of digitalisation are linked to processes that are fundamentally impacting modern society, which is why it is useful to understand the debates around risks and society (Curran, 2016, pp. 42–43).

2.1.2 Overview of risk definitions

After the introduction of the theoretical background of the risk society, it is crucial to examine the understanding of the term “risk”. That is of particular importance because the “traditional”

¹ Due to the limitations of this paper, the debates around individualism and class relations cannot be addressed. Nevertheless, it must be underlined, that this thesis does not give a full overview of Beck's' social theory and criticism around it, which is nonetheless relevant.

risk definitions will serve as a base for understanding current efforts to outline “digital risks” and link this to the digital risk society.

Firstly, it is pertinent to note, that there is no universally agreed-upon definition of what risks are (Aven & Renn, 2009, p. 1). The understanding of risks is dependent on the theoretical framework and perspective applied (Ekberg, 2007, p. 346). It is crucial to underline, that the debates around risks and uncertainties are based on how society perceives them, resulting in the understanding of risks being a product of its historical, political and social context (Bonß, 2022, p. 4).

Historically the term risk originated in early modern times, linked to cost-benefit calculations in maritime trade, which enabled a consideration of the benefits and threats linked to a transaction (Luhmann, 2003, pp. 18–19). Luhmann (2003) has noted, that risk can be characterised as “dealing with time”, which underlines that the term risk covers the attempt to calculate and deal with future uncertainties (Luhmann, 2003, p. 59).

This perspective is linked to the executions of Beck, who delimits his explanations from Luhmann’s elaborations of risks being tied to a calculating function (C. Schmidt, 2021, p. 14). Beck underlines, that the category of risk is expressed through “not being able to know”, which leads to risk rather being the handling of uncertainties, instead of purely a calculation of uncertainties (Beck, 2008, p. 22).

That is why Beck has defined risks as the following:

“Risk may be defined as a systematic way of dealing with hazards and insecurities introduced by modernization itself.” (Beck, 1992 (first 1986), p. 21).

This definition is of particular importance, because it highlights, that risks result out of modernisation and are thus manufactured (Jong, 2022, p. 6). Beck's definition of risks has been widely criticised (Aven, 2012, p. 1043). Campbell and Currie (2006) have illuminated in their criticism, that the above-mentioned definition of risks is problematic because risk itself cannot be a way of dealing with something, rather risks have to be something that is dealt with (Campbell & Currie, 2006, p. 151).

In Beck’s earlier work, the remarks on the terminology of risks are brought. Only a differentiation between risks (threats) and dangers is made. In that regard, the nature of risks is characterised as being controllable, whilst dangers are seen as being uncontrollable (Beck, 1999, pp. 310–319).

On this matter, it must be underlined, that the term “risk” and “threat” is often used synonymously. An important differentiation must be made, which illuminates the pre-assumption, that is linked to risks. Threats are characterised as something or someone that has the potential to cause harm, whereas the pre-assumption of risks is that they can cause harm, which is why they are characterised by the possibility of harm and the consequences that go along with the harm that is caused (Strachan-Morris, 2012, p. 173).

In the second book “world risk society” (2008) Beck alters his perspective by making an important differentiation between risk and catastrophe, underlining that the terms cannot be used synonymously. Risks are defined as the “anticipation” of a catastrophe and are characterised by the possibility of events or developments that do not exist yet (Beck, 2008, p. 29).

In that regard, the definition of the term risk is seen as a discourse (Beck, 2008, p. 66). This reveals that risks are seen as a social construction and based on definitions, that are negotiated. It is debatable if the understanding of risks in Beck’s work is a realist or constructionist perspective (Ormrod, 2013, p. 728). Nevertheless, this perspective on risk has been often located within critical realism, because risks are seen as an objective danger, that is mediated through social and cultural processes (Lupton, 2023, p. 45).

Giddens notes that *“There is no risk which can even be described without reference to a value [...]. When there is a clash of the different types of risk, there is a clash of values and a directly political set of questions.”* (Giddens, 1999, p. 5).

Risks are connected to aspects such as security, safety, and responsibility. Due to modern risks being manufactured, the question arises of what that means for responsibilities. Giddens states, that the manufactured risks go along with a crisis of responsibility (Giddens, 1999, pp. 7–8).

In the risk society, those aspects of risks are linked to a so-called “organised irresponsibility”, which the risk society results from. This concept describes that institutions cannot control the global risks of the risk society. That is the case because modern risks cannot be controlled by traditional institutions, as they are not equipped to deal with global risks based on their tools and methods for regulations and policies (Jong, 2022, p. 3). Beck argues, that modern risks lack accountability, due to their uncalculatable nature, which is based on global risks not being characterised by temporality or spatiality (Rosa et al., 2015, pp. 72–73). Hence, the question of accountability and responsibility in the context of risks is an important one to ask, as they are manufactured and based on actions and decisions (Bonß, 2022, p. 6).

Furthermore, risks are not only manufactured but also expanded into diverse dimensions of human life. Especially in the context of technology. In early theories around risks and society, technology and science were not seen as being the manufacturers of risks for society (Giddens, 1999, p. 4). This perspective is challenged by stating that risks are manufactured and are the consequences of technological use (Sundberg, 2023, p. 3). This underlines, that science and technology create uncertainties, which cannot be solved in a simple manner (Giddens, 1999, p. 4).

In the context of the risk society technology plays a central role, because it is linked to “decision-making power” (Sundberg, 2023, p. 3). Giddens (1999) has argued that this is particularly dangerous because the risks arising from the technological frontiers are linked to a lack of full understanding of the technology (Giddens, 1999, p. 3).

Aven (2012) has redefined the meaning of risks, based on Beck's approach and his own criticism against this approach:

“Risk refers to uncertainty about and severity of the events and consequences (or outcomes) of an activity with respect to something that humans value.” (Aven & Renn, 2009, p. 6).

This definition underlines the aspect of action in the context of risks. Risks require a subject-related decision for uncertainty. Due to risk dependency on action, risks can be characterised as a negative threat or as a positive chance (Bonß, 2022, p. 6). This aspect of the definition goes along with Becks and Giddens' arguments that modern risks are products of human decisions and thus, manufactured (Rosa et al., 2015, p. 72). Particularly in the context of this thesis, this perspective on risks is interesting, due to technological innovation often being linked to progress and “development” in a positive manner (Lupton, 2016, p. 304).

Because of this, it must be underlined, that in the field of risk management and risk analysis a “technico-scientific” approach to risks is employed, which focuses on probabilities, failing to address the nature of risks and how they are socially constructed (Lupton, 2023, pp. 25–26). For that reason, risks cannot be a function of probability and harm. That is the case because probability is rather “a tool to describe or measure uncertainties”, but not sufficient to characterise the concept of risk itself (Aven, 2012, p. 1044).

Rosa (2003) underlines that the states of risks are not predetermined, following in them being probabilistic and linked to a degree of uncertainty (Rosa, 2003, p. 56). That is why the following often-cited definition of risk is given: *“Risk is a situation or event where something of human value (including humans themselves) is at stake and where the outcome is uncertain.”* (Rosa, 2003, p. 56).

This definition will be used during this thesis because it aligns aspects, that many risk definitions have in common. Firstly, risk represents a state of reality of human concern or interest. Secondly, an outcome of the risk is possible and thirdly risk is linked to uncertainty (Rosa, 2003, pp. 55–56).

2.2 The Digital Risk Society

The overview of older debates around the risk society and the definitions of risks will now be extended to current debates around the digital risk society and digital risks. As already mentioned, the current research around digital risks and the digital risk society is limited (Sundberg, 2023, pp. 1–2). This is of particular importance, as the conducted research on digital risks for this thesis has revealed a marginal academic revival of the risk society and linked to this a potentially new emerging research field linked to the digital risk society. No research streams associated with the work around digital risks and the digital risk society can be identified in this thesis. Rather it seems like individual researchers are analysing digital risks out of their research fields, namely risk studies, legal studies, economics, sociology, and political science. This highlights the interdisciplinarity that the subject “risk and society” is aligned to. In that regard, there is no single research community, but rather scholars can be found in each discipline that works on aspects linked to the subject. Given this, it is hard to define a clear field in which risks and society are discussed (Alemanno, 2016, pp. 193–194). Nevertheless, recent publications have shown that a field linked to risks and society is emerging as a potential autonomous field. Moreover, the conducted literature review for this thesis has shown, that most current research on digital risks refers to the work of Ulrich Beck, which is why the risk society is being revisited and adjusted. International research cites his elaborations on risks, whilst at the same time being detached from his overall theoretical work (see Grenz, 2023; Lupton, 2016, 2023; Sundberg, 2023). That is why in the following Beck’s characterisation of digital risks will be extended by other more recent work around digital risks and the digital risk society.

2.2.1 Overview of digital risk definitions

The risks that are linked to technology and digitalisation are diverse. Particularly risks to society posed by digitalisation have not been studied to the fullest (Vinichenko, Nikiporets-Takigawa, Chulanova, & Ljapunova, 2021, pp. 108–109). That is why academic research does not give a universal definition or conceptualisation of digital risks (Dutt, 2023, p. 357). Nevertheless, in the following, an attempt is made to characterise and define digital risks.

Starting with Beck's latest work he highlights, that digital risks are linked to key features, that all global risks embody. Firstly, digital risks have a global nature, which underlines the global connectiveness within everyday life (Beck, 2017, pp. 186–187). Secondly, digital risks are the consequences that arise from a modernisation process. Those processes have been driven by institutions, which have lost stability due to the negative side effects of their actions. Nowadays for example the democratic control over technology by national states can be problematic (Beck, 2017, p. 187). Thirdly, digital risks are evaluated differently depending on the context and part of the world they exist in. Beck focuses on the so-called “digital freedom risks”, which are evaluated differently from global risks, due to their immaterial nature (Beck, 2017, p. 187).

From Beck's perspective the so-called “digital freedom risk” is one of the most important risks for modern society (Beck, 2014). In tradition with his arguments around the risk society, Beck states that digital risks go along with new inequalities, hierarchies, and structures for which traditional social categories such as class are not sufficient. That is why there is a need to analyse the new emerging structures with new analytical frameworks (Beck, 2014). As already mentioned in the part around the risk society, Beck has faced criticism for his call to replace traditional categories with new categories, that are mainly structured and centred around risks (see Curran, 2013, 2016; Knöbl, 2017).

Beck states that the beginning of the debates around digital freedom risks was characterised by a disparity between “*what the assumed and the actual state of data protection and freedom was within western society*” (Beck, 2017, p. 186).

This is connected to the paradox of digital risks, which Beck identifies. The closer society gets to a digital catastrophe, the less visible it gets. This argument is influenced by the events around the whistle-blower Edward Snowden. The NSA scandal has revealed that society was only able to find out about the governmental program, due to the whistle-blower. This illuminates, that the public is dependent on experts or whistle-blowers to find out about the digital risks (Beck, 2017, p. 186). This makes the awareness of the risk more fragile compared to other risks, which can be seen as another key feature of digital risks (Beck, 2017, p. 188).

Given this, the anticipation of the catastrophe is the important aspect, instead of the catastrophe itself. That is of particular importance because the anticipation of the digital catastrophe is seen as the only way, in which a space to counter it can open up (Beck, 2014). Those recent elaborations on digital risks are in line with Beck's traditional work on risks, in which risks are defined as the “anticipation” of the catastrophe and characterised by the possibility of events or developments that do not exist yet (Beck, 2008, p. 29).

His latest work on digital risks is linked to the problem, that digital risks are veiled due to their immaterial, global and complex nature (Beck, 2017, p. 186). Beck describes a “competition of risks”, because the different types of risks are intertwined with each other. For example, the risk of surveillance could be a response to the risk of terrorism. That is why institutions do not have the means to confront digital risks, such as “the risk of freedom of speech or the right to privacy” (Beck, 2014).

The outlined characterisation of digital risks will now be extended by more recent work on digital risks. Generally, digital risks are seen as a “lived-with concept”, that is linked to possible harm in the future (Curran, 2018, p. 208). Social and economic interactions have been affected and transformed by digitalisation processes, which have led to the emergence of digital risks (Ngwenyama, Henriksen, & Hardt, 2023, p. 108). Since the technologies that are linked to digital risks, such as artificial intelligence, are only emerging it is unclear if “digital risks are intrinsic” to the technologies (Galaz et al., 2021, p. 8)

Regardless, it can be noted, that digital risks are not only reproduced and mediated through technology, but also new digital risks are emerging out of the technologies themselves (Lupton, 2016, p. 301). It is crucial to underline that digitalisation and the rise of new technologies are not only linked to challenges to society but can also have positive effects on society (Vinichenko et al., 2021, p. 109).

Digitalisation can be defined as “*the way many domains of social life are restructured around digital communication and media infrastructures*” (Brennen & Kreiss, 2016, p. 1). Furthermore, digitalisation “*refers to the changes it leads to in technical, cultural, economic, ecological, ideological and societal spheres.*” (S. Schaefer, M. Andersson, E. Bjarnason, & K. Hansson, 2018, p. 11).

In that sense, the debates around digitalisation seem ambivalent. On the one side technology is seen as provoking innovation, solutions, and prosperity. On the other side, technology is linked to threats to democracy and security, manipulation and power asymmetries (Lupton, 2016, p. 304). Nonetheless, many optimistic perspectives around progress and advancement around the developments of technology have been shaping the debates around technology and society (Mouthaan, Frenken, Piscicelli, & Vaskelainen, 2023).

Against that background digital risks operate on different dimensions and thus have different implications, depending on the context they operate in (Dutt, 2023, p. 358). Therefore, it is important to differentiate between the dimensions digital risks operate in.

Because of this, Lupton (2016) has differentiated two different levels of digital risks operate in. First, digital risks that affect individuals and second digital risks that arise at a national or a global level (Lupton, 2016, pp. 304–305).

On an individual level, the use of technologies is linked to diverse digital risks, such as “*internet addiction, predatory behaviour by paedophiles online, the cyber-bullying of children, illegal activities on the “dark” web [...].*” (Lupton, 2016, p. 304).

On this micro level digital risks occur with direct or indirect effects on individuals who use specific services. Dutt (2023) has identified four categories in which digital risks on individuals could be grouped in (1) physical (2) financial (3) psychological and (4) social risks (Dutt, 2023, p. 358). Karwatzki, Trenz and Veit (2022) have assembled a multidimensional conceptualisation of privacy risks including “physical, social, resource-related, psychological, prosecution-related, career-related and freedom-related privacy risks” (Karwatzki et al., 2022, p. 1135).

This is linked to the macro level digital risks operate in and their implications for society. The risks for society are interwoven with the risks for individuals, such as the threat to democracy due to disinformation, fake news, surveillance, filter bubbles or online hate speech (Kuehn & Salter, 2020; Schünemann, 2022). Moreover, digital risks emerge out of dependencies on a global and national level. For example, security systems that governments and workplaces rely on can be at risk if the systems get attacked or fail to work (Lupton, 2016, p. 305).

Concluding based on the previous remarks, digital risks have an immaterial, global and complex nature. They are mostly veiled, which is why expert knowledge is needed to become aware of the risks. They arise out of digitalisation and the use of technology; thus, digital risks are a product of modernisation. Finally, digital risks can be seen as a lived-with-concept, which operates in different dimensions.

Based on the risk definitions by Aven and Renn (2009, p. 6) and Rosa (2003, p. 56) and the outlined characterisation of digital risks the following self-extended definition of digital risks will be used: *Digital risks refer to the uncertainty about a situation or event and the potential consequences (or outcomes) when something of human value (including humans themselves) is at stake because of digital technologies and the use of technology.*

2.2.2 Characterising the Digital Risk Society

In the following an attempt is made to grasp the current literature around the digital risk society, noting that only a few scholars have revisited the risks society and extended it to what could be

called a digital risk society. The starting point will be Beck's latest book "The Metamorphosis of the World" (2017), which was finished by his wife after he passed away in 2015. Based on this work it is possible to connect the current debates around digital risks with the older debates around the risk society (Knöbl, 2017, p. 1).

Beck (2017) uses the term "metamorphosis", which refers to a descriptive concept, stating that it is not normative, due to its non-directional and non-intentional notion (Beck, 2017, p. 33). From this perspective the world is not only changing but is rather in a state of "metamorphosis", meaning that the world is changing into something new. To be able to understand this process and grasp the structures of the present, the new must be analysed (Beck, 2017, pp. 15–16). In his latest argumentation, the risk society can be seen as the "actor" of the metamorphosis (Beck, 2017, p. 86). In that regard, it must be underlined that the conceptual work around the term "metamorphosis" is not developed to the fullest, which leaves it unclear what exactly the new is and how it can be differentiated from concepts, such as social change or transformation (Knöbl, 2017, pp. 4–5).

Beck proposes a cosmopolitical development of theory, stating that the traditional social theories are "end-of-history" sociology (Beck, 2017, p. 97). Underlining the difference between theory and time diagnosis, Beck illustrates that he is proposing a historical diagnosis, which is guided by theory (Beck, 2017, pp. 98–99). With his argumentation, he is in line with the tradition of modernisation theorists, who underline that the current developments of the present are linked to the beginning of a new era (Knöbl, 2017, p. 3).

Particularly in the context of digitalisation, this argumentation is interesting, due to the debates around the revolutionary potential of transformation processes caused by technology (Egard & Hansson, 2023, p. 763). Is technology changing the world to something completely new or is technology only adjusting to the old world? Those debates are especially present in the light of platforms and the emerging platform economy, which is changing economic and social structures (see Staab, 2021).

Beck identifies a "technological determinism" within modern society, in which technology and science are seen as progress, linked to mainly optimistic perspectives on technology (Beck, 2017, pp. 87–88). This technological determinism veils the power dimension, for example, the control over personal data is opaque because it is in the hands of private businesses and the state (Beck, 2017, p. 189).

Against this background, it is interesting to underline that "digital modernity" is characterised based on the overlap of the state, individuals and the private economy (Beck, 2017, p. 193).

Beck argues that a transnational digital class based on technology experts arises, which uses global digital risks as a source of power (Beck, 2017, p. 193). This is linked to institutional failure, which occurs because national solutions that are proposed by governments cannot keep up with the global nature of digital risks (Beck, 2017, p. 190). That is why for Beck the political and social order dissolves based on the digital metamorphosis (Beck, 2017, p. 194).

Hence, the metamorphosis of the world goes along with the simultaneous functioning and the failure of institutions (Beck, 2017, p. 185). Beck illuminates his argument with the example of digital freedom risks. As already mentioned, digital freedom risks are veiled and experts are needed for their identification (Beck, 2017, p. 186). In that context, Beck underlines that “*an anonymous digital central power is emerging that controls our private lives behind a democratic façade*” (Beck, 2017, p. 189). Looking at the developments of the past years and debates around technology and regulations, this argument must be seen critically. It is unclear to what extent there is control over our private lives, by whom and what interests of different actors stand behind the control over data. The argument lacks empirical evidence. Moreover, Beck's argumentations seem to be built in a normative way. Nevertheless, this hypothesis is interesting in the context of this thesis, which focuses on digital risks and the attempt of governments to regulate those risks.

Finally, the term digital metamorphosis refers to the merging of the online and offline spheres. The “digital human” that emerges out of this process is not necessarily linked to categories such as social status or social identity but rather to new categories (Beck, 2017, p. 191). As already mentioned in the first part Beck's arguments around categories such as class dissolving based on the new digital risks in modern society must be seen critically. Particularly in the context of digitalisation, many social inequalities can be identified that are linked to discrimination based on class, social status, or social identity (Lupton, 2016, p. 306).

Nevertheless, Beck finishes his last book by appealing to “digital humanism”, which must be established as a consequence of the developments. Based on this digital humanism data privacy and digital freedom must stand at the centre of emancipatory demands (Beck, 2017, p. 192). This goes along with what he called an “emancipatory catastrophism”, illuminating the transformative potential of the world risk society. This reconceptualisation towards the hidden emancipatory side effects is important, because “*emancipatory catastrophism is about the positive side effects of the bads*” (Rasborg, 2018, p. 165).

After the outline of Beck's elaborations on the current modern world and digital risks, the limited research will be introduced, that has revisited the risk society and adjusted it to a digital risk society.

Lupton (2016) has characterised the digital risk society based on three dimensions of risks (1) risks that are reproduced through technology and are thus a new source of risks (2) the use of technology, that poses risks (3) new social inequalities that result out of technology. It is argued that those dimensions of risks require new theoretical work on risks, which focuses on the intersection between technology and risks (Lupton, 2016, p. 301). This intersection of risks and digital technologies leads to “livelier” forms of risks in a digital risk society (Lupton, 2023, p. 38). Therefore, a new approach to the digital risk society is needed, moving away from traditional approaches of the risk society (Lupton, 2016, p. 301).

Additionally, the power dimensions of technologies must be highlighted for theorising the digital risk society (Lupton, 2023, p. 106). This is linked to the control over data, which enables surveillance on different levels. Moreover, an understanding of how computer coding and algorithms are structuring modern society needs to be established in the context of the digital risk society (Lupton, 2016, pp. 302–303).

Finally, the digital risk society is characterised by digital social inequalities, that are associated with on the one side the access and use of technology, on the other side the discrimination and bias that is coded into technological systems (e.g. algorithmic discrimination) (Lupton, 2016, p. 306).

Another perspective on the digital risk society can be found in the most recent work of Sundberg (2023), who has characterised the digital risk society based on an analysis of academic papers. The outcomes were, that in the digital risk society “(1) intangible technologies serve as solutions, whilst simultaneously introducing new risks (2) society is suffering from dehumanization, due to an increasing number of tasks, delegated to machines (3) scholars are calling for new approaches to govern these technologies” (Sundberg, 2023, p. 1).

Following Sundberg’s (2023) characterisation, the digital risk society is “layered”, due to the use of technology to solve problems that are caused by technology. Those risks can be understood as digital-self generated risks. Moreover, increasing standardisation of the use of data results in increased areas in which humans only engage with “digital artefacts” and are thus only users, which is linked to a process of “dehumanisation”. The relevance of technology for society and individuals’ daily lives is increasing, which is linked to calls for regulation. Privacy risks, surveillance by governments and risks related to the ownership of technology and

data are some of the reasons why new approaches are needed to address digital risks in the digital risk society (Sundberg, 2023, p. 10).

In conclusion, it could be argued that the debates around the digital risk society are only emerging and that the approaches and definitions vary, depending on the perspective employed. In the context of current digital risks and regulatory approaches future research is needed and the concept of the digital risk society needs to be expanded in an interdisciplinary manner. That is of particular importance, due to the relevance of digital risks and their regulation for society. Therefore, in the following the platform economy will be introduced and linked to digital risks, as this thesis employs a socioeconomic perspective.

3. The Platform Economy

Platform businesses, such as social media have become increasingly relevant to the public and private life. They are accompanied by transformation processes within the economy, society and politics (Poell et al., 2019, p. 1). That is why research on the platform economy is done within diverse disciplines, such as economics, business management, computer science and communication studies. This makes it difficult to give a holistic overview of the research that has been done. Due to the diversity in perspectives and different aspects, which are illuminated by the disciplines, this chapter cannot reflect the current state of research (Acs, Song, Szerb, Audretsch, & Komlósi, 2021, p. 1630). This thesis focuses on the way platforms are structured and function within the economy. That is the case, because in the later course of this thesis, a critical perspective on the way economic value is generated will be employed, highlighting how this affects the digital risk society. Against this background, the economic/ business perspective is highlighted in this chapter. First, the relevance of the platform economy will be presented, followed by a characterisation of the platform economy and its business models. The last part will focus on value extraction based on data and the technological means, which are employed. This part of the thesis is partly informed by previous research in the context of my Bachelor's Thesis in the studies of socioeconomic on the data economy and social inequalities (El-Aawar, 2020).

3.1 Introducing the platform economy

In 2020 the market capitalisation of the four big-tech companies Alphabet-Google, Amazon, Apple and Facebook made up to 5.7 trillion US-Dollars (Gawer & Srnicek, 2021, p. 4). The platform economy has quickly grown in revenue. In the EU the revenue grew from 3 billion euros in 2016, to 14 billion euros in 2020, highlighting the relevance of the platform economy

(Council of the European Union, 2023). Because of this, the European Union established an “Observatory on the Online Platform Economy” in 2018 in the course of their digital future strategy (Turillazzi, Taddeo, Floridi, & Casolari, 2023, p. 84). An expert group has published reports on platform power, which should “uncover blind spots in the policy debate on platform power” (European Commission, 2021). This highlights the relevance and awareness of dangers that could arise out of the platform economy.

Given this it must be underlined, that there is no universal agreed upon definition of the platform economy (see Liang, Aroles, & Brandl, 2022, p. 318). Generally, the platform economy refers to the rise of platform-based businesses and how they have transformed and created new markets (Khan, Zeng, Knight, Rajwani, & Pattnaik, 2023, pp. 1–2). Given this, new digital markets have emerged out of the platform economy (Schneider, 2018, p. 131). The platform economy can be seen as an overreaching term, which includes diverse economic models, such as the sharing economy, the collaborative economy, platform work and many more (Fuster Morell, 2022, p. 6).

Peticca-Harris et al. (2020) have defined the platform economy based on Belk’s (2014) elaborations as the following: *“The platform economy is made possible by new kinds of horizontal, networked exchanges and interactions between users through online communities. The platform economy is structured around ‘temporary access, non-ownership models of utilizing consumer goods and services [and often rely] on the Internet, and especially Web 2.0 [...]”* (Peticca-Harris et al., 2020, p. 37).

Thus the platform economy does not only describe the use of technology but also the emergence of new business models (Liang et al., 2022, p. 319). In that regard, the logic of the platform economy is not fundamentally new. Rather a traditional economic logic is employed, but in a different way (Goldfarb & Tucker, 2019, pp. 3–4). That is why it is important to highlight the new characteristics of the platform economy to be able to understand the logic behind the business models of the platform economy.

Montalban et al. (2019) have defined the platform economy as *“economic activities where tangible or intangible resources are exchanged between providers and users by the way of centralised electronic platforms.”* (Montalban et al., 2019, p. 807).

This definition highlights the matchmaking role and the rule-setting role of platforms, which underlines that the platform economy can be outlined based on the key characteristics of platforms, which will be illuminated in the following part (Montalban et al., 2019, p. 807).

3.2 Overview of platform definitions

Since the early 1990s digital business models have emerged and dominated diverse industries, forming the so-called platform economy (Xue, Tian, & Zhao, 2020, p. 1). It must be noticed, that the understanding of platforms varies and depends on which discipline is employed to understand the terms (Poell et al., 2019, p. 3). Nevertheless, the field of platforms has been heavily researched, which is why many definitions and concepts around platforms can be found. The conducted research has revealed that many definitions and concepts overlap and cover similar aspects, particularly in the context of economic value creation. Due to the limitations of this thesis, the current state of research cannot be presented in its entirety. In the following an attempt is made to elaborate the mostly cited definitions and authors from different disciplines, underlining that the claim is not to give a holistic overview, but rather to work out definitions and characterisations of the platform economy, which will help to answer the research question. For this thesis, the similarities within the definitions will be highlighted in bold. Moreover, the terms online platforms, digital platforms and platforms are used synonymously (Gawer & Srnicek, 2021, p. 2).

Gawer and Srnicek (2021) have defined platforms in their study on online platforms conducted for the European Parliament. Online platforms “*are **organisations** (that are most often, but not always, firms) that **offer digital services** that **facilitate interactions** via the Internet **between** two or more distinct but interdependent sets of **users** (whether organisations or individuals) and that generate and take advantage of network effects.*” (Gawer & Srnicek, 2021, p. 2).

The OECD has defined online platforms as “*a **digital service** that **facilitates interactions between** two or more distinct but interdependent sets of **users** (whether firms or individuals) who interact through the service via the Internet.*” (OECD, 2019, p. 20).

Those definitions are similar to the definition employed by Poell, Nieborg and van Dijck (2019). Based on their conducted research they have created a definition of platforms, combining the understanding of platforms in business studies and software studies. Thus, platforms are defined as “*(re-)programmable **digital infrastructures** that **facilitate and shape personalised interactions among end-users** and complementors, organised through the systematic collection, algorithmic processing, monetisation, and circulation of data.*” (Poell et al., 2019, p. 3). This definition combines perspectives on platforms of software and business studies, by underlining that digital infrastructures are programmed and linked to the business perspective of “two-sided markets”, which will be explained in the later course of this chapter (Poell et al., 2019, p. 3).

Those general definitions have similar aspects, as they focus on interactions between users (firms, organisations or individuals), which are enabled by the digital infrastructures and services that are offered. Platforms are seen as the intermediary of exchange between two or more participants (Xue et al., 2020, p. 1). That is why they can be characterised as non-human mediators (Peticca-Harris et al., 2020, p. 37).

Nick Srnicek (2018) has presented four key characteristics of platforms. First, they are **digital infrastructures**, which enable multi-sided interactions. Second, they produce **network effects**. Third, they use **cross-subsidation**, which means, that one service is provided for free, enabling revenues on another side. Forth, the **rules** are set by the platform owners (Srnicek, 2018, pp. 46–50).

In the following, the characterisation of platforms as digital infrastructures will be illuminated briefly noting, that the complex debates around infrastructures will not be mapped out. It is debated whether or not platforms can be characterised as digital infrastructures, particularly from a legal perspective (Hesmondhalgh, Valverde, Kaye, & Li, 2023, pp. 296–297). Digital infrastructure can be defined as *“a socially embedded mechanical system that includes technological and human components, network, systems, and processes that generate self reinforcing feedback loops.”* (Acs et al., 2021, p. 1638). Feedback loops mean, that the use of data (or the use of revenues from the use of data, such as advertising) enables an improvement in the quality or value of a business (Szczepański, 2020, p. 5). The terms platforms and digital infrastructures are often used as synonyms (Grenz, 2023, p. 99). Both infrastructures and platforms have diverse characteristics in common but at the same time some differences in their scale and scope (see Plantin, Lagoze, Edwards, & Sandvig, 2018). Tucker (2021) has argued, that it is not evident, that platforms such as Uber, Google or Wikipedia can be defined as infrastructure. Rather she argues that the claim that digital platforms are infrastructures emerges out of the platforms themselves, by imposing the claim on their users (Tucker, 2021, p. 450). This argument is interesting and worth noting because it underlines that platforms are systems, which are linked to power dimensions.

Recognising the debates around whether or not platforms can be seen as digital infrastructure, it is important to underline that platforms have become a crucial part of individual's lives and society, which are linked to characteristics like infrastructures. In this sense, digital infrastructures have become a layer of the social and are linked to economics, politics, and society. The growing relevance for society and entanglement into diverse areas of society go

along with digital infrastructures becoming more and more complex to understand (Grenz, 2023, pp. 98–99).

Secondly, online platforms are characterised as multi-sided markets, which are linked to network effects (Acs et al., 2021, p. 1635). Particularly in business studies have analysed platforms through the lens of markets (Poell et al., 2019, p. 5). Within those disciplines, the elaborations by David Evans (2003) on platforms and two- or multi-sided markets have been widely cited. He defines multi-sided platforms as *“a market, which coordinate the demands of customers, who need each other in some way”* (Evans, 2003, p. 325). Platforms provide goods or services to distinct groups, who rely on the platform as an intermediary. Platforms minimise the transaction costs, which is a key factor for the value creation in the platform economy. Platforms reduce the costs of finding and searching, by so-called “match-making” (Evans, Schmalensee, Noel, Chang, & Garcia-Swartz, 2011, p. 137). Moreover, digital platforms are characterised by their global nature, because geographic boundaries are less relevant for the digital markets (Gawer & Srnicek, 2021, p. 12).

Platforms operate with different economic rules. Traditional businesses for example buy material, process this material, and sell the output. For platforms, the raw materials are the groups they match and data linked to the groups, which is why the infrastructure for matchmaking is the marketplace where the value is generated (Evans & Schmalensee, 2016, p. 1). This new emerging market is linked to necessary conditions that must be met by the platform businesses: (1) two or more distinct groups of customers must be present (2) external effects arise when two groups of customers are connected or coordinated (3) an intermediary is necessary to internalise the external effects (Evans, 2003, pp. 331–333).

Platforms are linked to **direct** and **indirect network effects**, which describe the value that is generated out of the interactions, which take place (Acs et al., 2021, p. 1636). Direct network effects are generated out of the number of users. This is particularly true for online platforms, such as social media the case. On the one side, the direct network effects describe that the benefits for users depend on the number of other users they interact with. On the other hand, indirect network effects arise when different stakeholders of the platforms can benefit from the size and characteristics of the “other side” (the users). The example of streaming platforms makes the explanation more comprehensible. A streaming platform is valuable for its users if the offer and range of videos are high, those are the direct network effects. On the other side, the indirect network effect arises out of the number of users that the platform has. Due to the large user-base, the streaming service becomes valuable for stakeholders, such as content

creators, movie studios or advertisement firms, to also participate on the platform (McIntyre & Srinivasan, 2017, p. 143). Thus, “*more sellers attract more buyers, and more buyers attract more sellers*” (Acs et al., 2021, p. 1636).

Based on those network effects, platforms become powerful, because they can dominate markets. This is linked to so-called “**lock-in effects**”, which describe that the cost of switching a platform becomes higher, the higher the network effects are. For example, the “costs” of not using WhatsApp as a messenger, when everybody uses WhatsApp becomes high, which makes it hard (but not impossible) for competition to enter the market (Schneider, 2018, pp. 131–132). That is why economic literature suggests a “**winner-takes-it-all/most**” principle, which is characteristic of the platform economy (McIntyre & Srinivasan, 2017, p. 144).

Thirdly, platforms are characterised based on **processes of cross-subsidation**. As already noted, the demand on one side is dependent on the volume of users on the other side (multi-sided character). In that regard subsidising one side leads to more users on the other side. For example, the free service of Facebook attracts more users, which then attracts more advertisement firms willing to pay for advertising on Facebook (Gawer & Srnicek, 2021, p. 13).

Finally, platforms are linked to **power dimensions**, which arise out of the characteristics mentioned. The power of platforms is not only limited to the economic market perspective (see Busch, Graef, Hofmann, & Gawer, 2021). Platforms have become self-regulatory environments, due to them operating based on contractual terms. The reason for this is the “membership agreement” that individuals must commit to when joining a platform. The rules are set out in the terms and conditions that the platform determines (Rodríguez de las Heras Ballell, 2021, p. 82). Rodríguez de las Heras Ballell (2021) has pointed out, that this is problematic not only due to legal issues but also due to power asymmetries arising from the self-regulation of platforms (Rodríguez de las Heras Ballell, 2021, p. 82). This aspect is linked to the dependency on the services and infrastructure, which the platforms provide. The higher the network and lock-in effects get, the more the power solidifies (Schneider, 2018, pp. 131–133).

Following Saadatmand, Lindgren, and Schultze (2019) digital platforms can be characterised as “*an emergent **organisational** form characterised by (1) **technology**: a technological architecture constituted of a modular core, standardized interfaces, and complementary extensions, and (2) **social processes**: a set of governance mechanisms to manage an ecosystem of independent complementors who complete the platform’s value proposition by co-creating its value.*” (Saadatmand, Lindgren, & Schultze, 2019, p. 1).

This definition highlights the aspect, that platforms create **platform-based ecosystems**, which are connected to the power dimensions. Those are characterised by their global nature and big scale in participants (users and agents). Ecosystems in that context refer to the way in which multiple services are interconnected and offered to users (Busch et al., 2021, p. 13). The governance of those ecosystems is mainly dominated by the platform owners themselves because they set the rules on who can participate and under what conditions (Acs et al., 2021, p. 1636). Moreover, the two-sided markets are linked to the accumulation of capital and power due to the monopoly of a few platform businesses (Poell et al., 2019, p. 5). Therefore, power arises out of the fact that platforms act as private regulators of their ecosystem (Gawer & Srnicek, 2021, p. 11).

Regarding the power dimensions, the discourse around platforms must be highlighted. Gillespie (2010) has underlined how the term platform is used to shape public discourse (Gillespie, 2010, pp. 347–348). Due to the supposed neutrality of technology, the term is sometimes employed to veil the agency of platforms (Plantin et al., 2018, p. 297). The way the term platform is used underlines “the claims about what those technological services are and what not, and linked to this what should be expected from them and what not” (Gillespie, 2010, p. 359).

That is why platform power is linked to “contractual” power on the one side, but also “artifactual” power on the other side. Artifactual power describes that power arises out of the software and algorithms because they have structuring effects. That is the case because the coding of algorithms or automated content management of the platforms can determine and affect user engagement (Kenney, Bearson, & Zysman, 2021, p. 1455).

In summary, online platforms are characterised based on their scale and scope, network effects, cross-subsidisation, lock-in effects, ecosystems they create, power based on the dependency on their services and the determination of markets and rules.

3.3 Value in the platform economy: the drive for data

The attempt to characterise platforms in the previous chapter has touched upon the value creation within the platform economy. The emergence of new business models has resulted in data-dependent markets. Against this background, data has been titled “the new oil”, which highlights that data has become a key resource of the modern economy (Szczepański, 2020, p. 1). Given the research question and the relevance of data for platform-based businesses, it is of particular importance to ask how value is derived from (personal) data (Sadowski, 2019, p. 6). It is of particular importance to illuminate the economic and business perspective on value

creation because it reveals information about the logic and structures of the platform economy. That is why in this chapter firstly the already mentioned value, which arises out of the platform's key characteristics will be outlined in more detail. This will be followed by highlighting how value is extracted based on personal data. In this chapter, only the key mechanisms will be outlined. That is the case because in the later course of this thesis, those key mechanisms will be extended by using the example of social media as data-driven business models of the platform economy.

As already mentioned digitalisation and the use of technology are linked to a transformation of the way economic value is generated (Gawer & Srnicek, 2021, p. 13). The value creation of modern platform businesses is embedded in the use of technology (Acs et al., 2021, p. 1636). Online platforms focus on their **core competencies** as intermediaries by providing digital services or digital infrastructure. This **specialisation** leads to the maximisation of profits (Chen, Li, Wei, & Yang, 2022, p. 1808). As already described in the previous part platform businesses are characterised as intermediaries or matchmakers. This aspect highlights that the value of digital platforms arises out of the fact that they reduce or **eliminate information costs** (Acs et al., 2021, p. 1636).

Moreover, economies of scale and scope arise, due to the **low cost of expansion and additional users** (Gawer & Srnicek, 2021, p. 12). This economic process can be explained with Jeremy Rifkin's (2015) elaborations on the modern economy. He outlines, that the modern economy is characterised by **zero marginal costs**, which is enabled using technology. The reason for those zero marginal costs is, that the production costs for an additional good or service are close to zero in the modern economy (Rifkin, 2015). Thus, platform businesses make high investments in the early stage of building their digital structures, which is followed by a rapid expansion at near-zero additional costs after the digital service is established (Gawer & Srnicek, 2021, p. 12). Furthermore, platforms create value out of the **ecosystems** they create (Kenney et al., 2021, p. 1454). McIntyre and Srinivasan (2017) have underlined, that the transaction, which online platforms enable, would not be possible without the platforms (McIntyre & Srinivasan, 2017, p. 141).

The new economic value, which is generated by platform businesses can be characterised as so-called "disruptive innovation". This describes the disruption of the economy based on new emerging digital businesses. Disruption in that sense is understood as a drastic transformation of markets, which leads to the emergence of new markets (OECD, 2019, p. 24).

So far, the economic value which is generated based on the key features of the platforms has been outlined, neglecting the **economic value of data** in this context. The new emerging markets and platform-based businesses are centred around data (Srnicek, 2017, pp. 254–255). The research on data-driven business models is still limited and needs further investigation (Zambetti et al., 2023, p. 208). Nevertheless, in the following, an attempt is made to illuminate the value of data and how (personal) data is being used by platforms.

Data-driven business models use data as a key resource for profit. Platforms **collect, extract, and analyse** data (Srnicek, 2017, pp. 254–255). The “data-drive” of the platform economy highlights that businesses are not only profit-driven but also data-driven, meaning that their function is linked to the accumulation of data. That is why the profit of business models of the platform economy is deeply interwoven with the monetisation of data (Sadowski, 2019, p. 1). In that regard, data is not available to every company in the same way. Rather the limited access to data, due to few businesses having a gatekeeper position, makes data an “excludable resource” (Lohsse, Staudenmayer, & Schulze, 2017, p. 15). Moreover, this position enables them to generate and access large amounts of data, which are facilitated on the platform (Busch et al., 2021, p. 10).

In general terms, data can be understood as *“forms of information that have been collected and processed using digital technologies [...]”* (Lupton, 2020, p. 44). This data has different properties, which makes it valuable (Krotova, Rusche, & Spiekermann, 2019, p. 9). The profits and economic performance of data-driven businesses depend on the availability, timeliness, and quality of data (Breidbach & Maglio, 2020, p. 168). Real-time data for example is more valuable to a company than “older” data (Krotova et al., 2019, p. 9). In that regard, data is very heterogeneous (Body of European Regulators for Electronic Communications, 2019, p. 106).

The evaluation and determination of the value of data is complex. There is no agreed-upon assessment system of how to define the value of data. In most cases, data-driven businesses have their own evaluation systems, which determine the price for the data or information if sold (see Krotova et al., 2019, p. 22).

Mejias and Couldry (2019) have characterised data as a commodity, because profit is generated out of the sale of data or the information that is extracted out of the data (Mejias & Couldry, 2019, p. 5). In contrast to this Sadowski (2019) has highlighted, that it is debatable if data can be seen as a “commodity” or as “capital”. This thesis will not outline the debates linked to this question. Nevertheless, this underlines that data has become a key factor for value creation, especially in the context of the neoliberal platform economy (Sadowski, 2019, p. 2).

Data can be categorised either into two categories (1) personalised or (2) non-personalised data. Non-personal data are for example information about time, the weather or viewing numbers. This type of data can also create economic value if clustered. In contrast, personal data gives detailed information about an individual, such as age, sex or nationality (Riesenhuber, 2019, pp. 36–37). Data-driven business models, especially social media platforms generate most of their profit by analysing and using personal data (Wessels, Laubach, & Buxmann, 2019, p. 13). That is why this thesis will focus mainly on personal data, as it has particular relevance in the context of the digital risk society and the Digital Service Act.

The EU has defined personal data in the General Data Protection Regulation (GDPR) article 4 no.1 as the following: *“personal data” means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.*” (European Union, 2016, p. 33).

The value does not arise from the data itself, but rather from the **information** that is extracted after processing the data (Huhtala, 2019, p. 56). This information can be duplicated and transported at low costs (Daum, 2019, p. 43). That is why personal data itself is economically valuable because it allows detailed information about an individual (Riesenhuber, 2019, pp. 36–37). Given this information and knowledge derived out of data have become a key resource for the modern economy (Acs et al., 2021, p. 1633).

If trying to understand where the value of data comes from it is important to ask where the data comes from in the first place. In most cases, data results as a by-product of the interaction in the digital spheres (human-to-human, human-to-machine or machine-to-machine interactions) (Breidbach & Maglio, 2020, p. 165). Breidbach and Maglio (2020) highlighted, that the “true” value of data and how data is generated is mostly veiled by the platforms because they need to ensure that data is generated, which they can use for profit (Breidbach & Maglio, 2020, p. 168). Particularly in the case of social media, a large amount of value is based on user-generated content (Chen et al., 2022, p. 1806).

In view of this data can be used for the business's own purposes or sold on so-called data-markets, which are untransparent and complex markets (Bründl, Matt, & Hess, 2016, pp. 67–68). For example, data can be sold to third parties, such as advertisers, which want to reach a specific target group (Lupton, 2020, p. 8). The sharing of data by platform providers in mostly

not transparent, particularly not for the users of the platform (Breidbach & Maglio, 2020, p. 175). As outlined some platform businesses sell data packages directly. Nevertheless, most platform businesses, especially social media platforms use the information for in-house purposes and do not share it, because of legal issues, especially in the context of personal data. Most regulations and laws around data protection prohibit the sharing of data, which would allow the identification of a natural person. That is why instead of selling the data directly, most platform businesses offer advertisement spots or information on target groups, based on the already analysed data, without given full access to the data (Lohsse et al., 2017, p. 15; Lupton, 2020, p. 8).

Sadowski (2019) has outlined five key ways, in which data generates value “(1) *data is used for profiling and targeting individuals* (2) *data is used to optimise systems* (3) *data is used for management and control* (4) *data is used to model probabilities* (5) *data is used to build digital systems.*” (Sadowski, 2019, p. 5-6).

This outline will be extended in the later course of this thesis. Nevertheless, a short introduction on how personal data is being used for advertisement and what type of technologies are involved will be given.

Personal data can be and is already getting used in many ways, such as creating user profiles which enable targeted advertisement, setting social norms and regulating citizens, based on biometric software, for surveillance cameras or “social credit systems” in China (Lupton, 2020, p. 9). As already mentioned personal data is mostly getting used for advertisement, because it enables a specific targeting of users (Huhtala, 2019, p. 55).

What type of information can be extracted from personal or genetic/biometric data has been outlined by the General Data Protection Regulation (GDPR) of the EU article 9 no. 1 “[...] *personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership [...]*.” (European Union, 2016, p. 38). Moreover, the GDPR highlights, that genetic or biometrical data can lead to the identification of a natural person, health information, information on a person’s sex life or sexual orientation (European Union, 2016, p. 38).

In view of this personal information is used by platforms to personalise user’s experience on the platform, enabling business companies to directly target users as consumers. That is why, companies have to use personal data in the platform economy, because otherwise, they would risk losing a competitive advantage (Huhtala, 2019, p. 56) This is done by curating the

information, which is presented to the users, based on their individual preferences and tastes, which are extracted from the personal data (Trzaskowski, 2022, p. 449).

The increased personalisation of the digital world has been linked to concerns related to “filter bubbles” and “echo chambers”, such as discrimination, algorithmic bias and radicalisation (see Möller, 2021; Pariser, 2012; Ross Arguedas, Robertson, Fletcher, & Nielsen, 2022). Those aspects will be discussed in the later part of this thesis.

Personal information is used to create digital profiles of users, which allow a prediction of their behaviour (Zuboff, 2019, pp. 65–66). Given this, so-called “predictive analysis” is employed by platform businesses. Siegel (2013) has defined predictive analysis as the following: *“Technology that learns from experience (data) to predict the future behaviour of individuals to [...] decisions.”* (Siegel, 2013, p. 11). The term “data mining” is often used synonymously with predictive analysis (Siegel, 2013, p. 12).

Hence, predictive analysis describes a process, in which personal data is used to understand the characteristics of an individual. Those characteristics function as the “input” for the prediction of human behaviour, which describes the output. In that regard, the data is processed by machine learning to build the prediction model (Siegel, 2013, pp. 26–27).

For processing and analysing the raw data **algorithms**, **artificial intelligence** and **machine learning** are used (Breidbach & Maglio, 2020, p. 164). The exchange on platforms is organised by algorithms, which collect and analyse data (Montalban et al., 2019, p. 807). Mahmud, Islam, Ahmed and Smolander (2022) have defined algorithms based on their conducted literature review as *“an automated process that provides decisions independently without the mediation of a human [...] (and) algorithms use data, statistics, and/or computing resources to make decisions.”* (Mahmud et al., 2022, p. 2).

Algorithms are constructed out of programmed search, sort and combination rules, determined by the programmer. Algorithms identify data sets, evaluate, and connect them based on the rules, which result in automated decision suggestions. Therefore, the output of an algorithm is based on probability (Prinzing, 2019, p. 271).

Algorithms use artificial intelligence and search for correlations, providing the base for future predictions (Breidbach & Maglio, 2020, p. 173). In this context, so-called “deep learning” has been employed within machine learning, which describes that the capabilities of algorithms to make decisions are developed “unsupervised”. This leads to humans not being directly involved in the development process because AI is used. This has ethical implications and is susceptible to undiscovered errors and bias (Breidbach & Maglio, 2020, p. 173). Based on deep learning

automated decisions are made, which can therefore be also characterised by a lack of human involvement in the decision-making process (Araujo, Helberger, Kruikemeier, & Vreese, 2020, p. 611). Araujo et al. (2020) have conceptualised automated decision-making as *“instances in which algorithms or an AI are used to collect, process, models, and use data to make automated decisions.”* (Araujo et al., 2020, p. 612).

Based on those mechanisms algorithms “guess” what information users want to see. This prediction is based on the information that has been gathered about a user, including information on geographical position or interests based on past click behaviour or search history (Schneider, 2018, p. 134).

Finally, not only the technology used to analyse data but also the technology used to structure the platform, such as the design plays a role in the data-driven value creation.

Following Riesenhuber (2019) the main profit of data-driven business models is generated out of the data that the users generate or their **attention**, particularly in the context of advertisement (Riesenhuber, 2019, p. 30). Therefore, the monetisation of attention is characteristic of the value extraction in the platform economy (Trzaskowski, 2022, p. 450).

This is linked to the design of the platforms, specifically the interfaces (Schneider, 2018, p. 131). The **technological architecture** includes the core, interface, and complementary modules, which enable the core functions. The core, which is for example part of the technological system, describes the hidden layer of the architecture, whilst the interface describes the digital infrastructure, that is visible to the public (Saadatmand et al., 2019, p. 4). Since data is generated based on interactions, which could be for example the viewing of a short video, the goal of the platforms is to keep the users as engaged and as long as possible on the platform. The way the interface and the infrastructure of the platform are designed is linked to this goal (Zeng, Abidin, & Schäfer, 2021, p. 1363). Thus, the value of platforms is driven by their architecture and the specifications of their interfaces (McIntyre & Srinivasan, 2017, p. 143).

In conclusion, the outlined value creation within the platform economy has underlined that the monetisation of data is based on transforming data into useful information for the platform businesses. This is done based on the use of technology, such as algorithms and AI (Azkan, Spiekermann, & Goecke, 2019, p. 62).

4. The Digital Service Act

The calls to regulate digital platforms have grown over the past years, due to an increased

awareness of the risks that platforms, mostly social media platforms pose for society. In the early years, intermediary platforms were linked to perspectives of free online speech. Thus, platforms were seen as facilitators of democracy, due to a reinforced public discourse (Heldt, 2022, p. 69). Those perspectives have changed, due to the way those platforms have developed and transformed in recent years (Rodríguez de las Heras Ballell, 2021, pp. 75–76). Particularly events that affected the European Union, like the voter manipulation through Facebook in the context of the UK Brexit campaign, hate speech against refugees in Germany and disinformation during the elections in 2017 in France have affected the discourse within the European Union (Heldt, 2022, p. 70). The developments of the past years have therefore raised concerns regarding the transparency and accountability of online platforms (Kalbhenn, 2021, p. 49).

Against this background national laws in Germany, Austria and France have been formed, which is why the European Union did not only react to the calls for regulations but also to the need to harmonise the different laws so that the standards across the EU become homogenous (Kalbhenn, 2021, p. 49). Legal harmonisation is of particular importance in the context of digitalisation as fragmentation leads to a less effective way to protect fundamental rights (Chiarella, 2022, p. 36). This harmonisation process is characteristic of the political and economic integration process of EU member states into the European Union and is linked to societal change within the member states (Worschech, Eig Müller, & Büttner, 2022, p. 15). Harmonisation means that the national regulations are levelled to a common ground, enabling a European integration process, which is characteristic of regulatory approaches (Börner, 2022, p. 240).

In that respect, the European Union has enacted the so-called “Digital Service Act” (DSA). The DSA requires “Very Large Online Platforms” (VLOPs) and “Very Large Online Search Engines” (VLOSEs) to become active parts of digital risk mitigation, as their systems are posing risks to society and individuals (Loi, 2023, p. 3).

In the following the Digital Service Act will be presented, using a mixture of literature, especially from law studies. It must be underlined that in this chapter many parts are directly cited from the law and European Commission’s website, due to the complex nature of EU regulations and the particularity of the legal language. Furthermore, the Digital Service Act will not be covered to a full extent, due to its length and complex content. Only an overview is given, focusing on Very Large Online Platforms and their obligations as the case studies used in the later part of this thesis can be characterised as VLOPs.

4.1 Towards a Digital Service Act

Digital services have become more and more important in the past years. This development went along with many societal challenges. Governments and International Institutions could not keep up with the rapid transformations linked to digitalisation, which is why a new set of rules was urgently needed. Especially in the context of the European Union this was the case because rules governing digital services have remained mainly unchanged, since the “e-Commerce Directive” in 2000 (Madiaga, 2022). This directive served as the foundation of the EU's strategy on digital services. Despite its importance, the e-Commerce Directive became outdated over the past years, due to some shortcomings such as a lack of harmonised application by the EU member states and a transformation of digital services, which enables the new emerging platform models to bypass the regulation and the creation of new legal issues (Rodríguez de las Heras Ballell, 2021, pp. 75–80).

Nevertheless, since 2016 the European Commission took actions to keep up with the rapid developments of digitalisation, which led to the DSA. In the early stages of 2016 “Online Platforms and the Digital Single Market Opportunities and Challenges for Europe” were highlighted (European Commission, 2016). The outlined challenges and opportunities were first met by the establishment of an observatory to the platform economy in 2018 to supervise its development and the Platform-to-Business Regulation from 2019 (Turillazzi et al., 2023, p. 84).

Those efforts were followed by the Digital Service Act and the Digital Markets Act (DMA), for which the process started in 2020. The two acts can be seen as a large package, that forms “a single set of rules” that should ensure the creation of a safer digital space, in which fundamental rights are protected whilst establishing a market that fosters innovation, growth and competitiveness (European Commission, 2023c).

The DSA sets out rules for a “safe, predictable and trusted online environment” (Duivenvoorde & Goanta, 2023, p. 5). The European Commission has stated clear goals of the DSA. For this thesis, the goals for (1) citizens and (2) society at large are mostly relevant (European Commission, 2023b).

First, for citizens, the DSA should enable a “*better protection of fundamental rights, more control and choice, stronger protection of children online and less exposure to illegal content*” (European Commission, 2023b). For society at large “*greater democratic control and oversight over systematic platforms and the mitigation of systematic risks, such as manipulation or disinformation*” are identified as overall goals (European Commission, 2023b).

The Digital Markets Act on the other side, should ensure “fair and open digital markets” by setting out rules on how large platforms, that act as “gatekeepers” should behave (European Commission, 2023a). It is important to underline that the DSA and the DMA are seen as a package and thus complement each other (European Commission, 2023c).

The DMA and DSA can be contextualised by the traditional categories around EU regulations. Usually, regulations are categorised either into *social regulations* or *economic regulations*. Social regulations address concerns related to for example health, safety, or consumer protection, whilst economic regulations cover activities in specific industries with monopolistic tendencies (Alemanno, 2016, p. 197). The package of the DSA and the DMA could be located within those two categories based on the explanation above. The DSA covers consumer protection and is concerned with risks to society; hence it can be characterised as a social regulation. In contrast, the DMA is concerned with the role of online platforms as gatekeepers, which would enable a characterisation as an economic regulation. This is important to underline as it shows that the package can be characterised as a “socioeconomic” regulation. That is why the object of the regulations is attributed to regulating risks based on market failure, which is directed towards protecting society from risks (Alemanno, 2016, p. 198).

This is linked to the overall digital strategy of the European Union. Under the headline “Shaping Europe’s digital future” the EU is working on strategies and policies regarding the digital transition. Against that background digital solutions that are centred around “putting people first” are the main goal of the efforts. The digital solutions are supposed to enable new business opportunities, encourage trustworthy technology, foster a democratic society, enable a sustainable economy and help to fight climate change and a green transition (European Commission, 2020b).

The digital strategies go along with reducing the dependency on countries outside of the EU that provide crucial technologies (European Commission, 2020b, p. 2). In 2020 online platforms from the EU only accounted for 2,7 % of the global total value, due to most of the EU’s platforms still being start-ups. Only 12 companies from the EU are in the global top 100. The value of the top 100 has increased in 2020 up to 40 % to 10,5 trillion Euros, which shows how important the digital economy has become (European Commission, 2019).

As Turillazzi (2023) puts it this is of particular importance and helps to understand the reasoning for the DSA and DMA package. In the EU a high level of fragmentation can be identified when it comes to the digital economy and relevant platform businesses. Many are still in development and cannot keep up with big global players. Concerning the DSA it must

be illuminated, that there is a clear trade-off between user protection and fostering innovation and competitiveness of online platforms within the European Union (Turillazzi et al., 2023, pp. 85–86). This reflects the tension between the need to protect fundamental rights in the economic sphere of online platforms, which has been private to them, whilst ensuring innovation, competition and development in the digital sector (Cauffmann & Goanta, 2021, p. 759).

Against this background, the European Commission proposed the DSA in 2020. The proposal highlights, that digital services are affecting and changing the daily lives of EU citizens, whilst transforming social and economic processes within the European Union and worldwide. Those services have become sources of new risks for individuals who are using those services and for society itself. That is why the European Commission has committed to updating the rules on the responsibilities and obligations of digital services (European Commission, 2020a).

After the legislative process, which will not be explained in this thesis, the final vote was taken in 2022, in which the Digital Services Act was adopted with a majority in favour (539 votes in favour, 54 votes against and 30 abstentions) (European Parliament, 2022b).

4.2 The Digital Service Act

4.2.1 Scope and scale of application

The DSA was published on the 27th of October 2022 and came into force by the 16th of November 2022 (European Commission, 2023c).

The DSA is an EU Regulation, which is defined as the following: *“Regulations are legal acts that apply automatically and uniformly to all EU countries as soon as they enter into force, without needing to be transposed into national law. They are binding in their entirety on all EU countries.”* (European Commission, 2023d).

That is why the DSA is directly applicable on the 16th of February 2024, 15 months after its publication. EU regulations can be seen as “horizontal” instruments, which means that they will coexist with other laws, such as the General Data Protection Regulation (GDPR) and other regulations on intellectual property and consumer protection (Husovec & Roche Laguna, 2022, p. 2). It is crucial to underline that the EU regulation does not only apply to European companies but rather to all companies that fall into the scope of application, regardless of whether or not the companies were established in the EU (Turillazzi et al., 2023, p. 86).

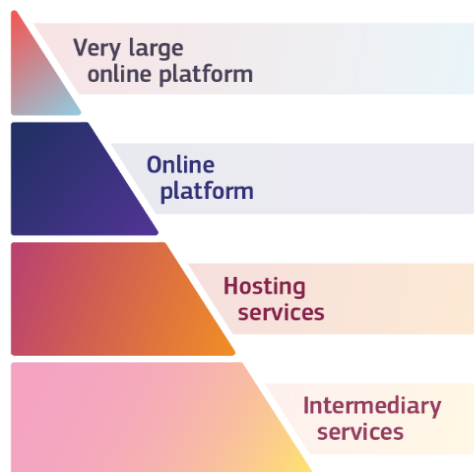


Figure 1 Providers covered by the DSA (European Commission, 2023b).

The DSA differentiates different types of online services (intermediary services, hosting services, online platforms, and very large online platforms). Those services are deeply intertwined with each other (see **Figure 1**). Hence intermediary services can be seen as the upper level, offering network infrastructure, such as Internet access providers. Intermediary services include hosting services, which represent the second level and are cloud or web hosting services, which include two other

categories, namely online platforms, and Very Large Online Platforms. Online platforms represent online marketplaces, like app stores or social media. Very large online platforms are also online platforms but characterised by their size, which in this context is based on the user numbers. Thus Very Large Online Platforms are defined as online platforms with more than active 45 million users, like Facebook or TikTok for example (European Commission, 2023b). Following Turillazzi (2023) those different categories are relevant because different obligations go along with the different types of categories a digital service falls into (Turillazzi et al., 2023, p. 86).

The focus of this thesis will be on Very Large Online Platforms (VLOPs), because of their relevance in the context of the digital risk society and thus the chosen case studies for this thesis, which can be characterised as VLOPs. That is why which is why the specific elaborations on Very Large Online Search Engines (VLOSEs) in the DSA will be excluded from this thesis. Online platforms are defined in Article 3 (i) as the following: “*a hosting service that, at the request of a recipient of the service, stores and disseminates information to the public [...].*” (European Union, 2022, p. 43).

Online platforms are required to publish their numbers of active users by the 17th of February 2023. This is relevant for the classification as Very Large Online Platforms or Very Large Online Search Engines. If the platforms have more than 45 million users, which is the equivalent of 10 % of the European population, the European Commission will classify the platforms as either VLOPs or VLOSEs. As a first step, those platforms have to comply with the obligations of the DSA (e.g. the first annual risk assessment) within 4 months. From the 17th of February onwards also platforms with less than 45 million active users have to comply with the DSA (European

Commission, 2023c). In that regard it must be underlined, that the scope of application is not fully clear, due to the broadened definition of users, being “active recipients of services” (Husovec & Roche Laguna, 2022, p. 9).

The Commission has published a list with 19 designated VLOPs, including AliExpress, Amazon Store, AppStore, Booking, **Facebook**, Google Maps, Google Play, Google Shopping, **Instagram**, LinkedIn, Pinterest, **Snapchat**, **TikTok**, Twitter, Wikipedia, YouTube and Zalando (European Commission, 2023b).

The marked platforms will be discussed in more detail manner in the later course of this thesis, specifically in Chapter 6.

4.2.2 Due diligence obligations

The DSA defines the accountability of the different digital services through their due diligence obligations (Decarolis & Li, 2023, p. 6). In the following, an overview (see **Table 1**) of the due diligence obligations that the DSA imposes will be given. The subject matter defined in Article 1 no. 2 (b) highlights, that different obligations are tailored to the different digital services, depending on the category they fall into (European Union, 2022, p. 41).

VLOPs have the most specific obligations to comply with but also have to comply with the obligations that apply to the other types of services (intermediary services, hosting services and online platforms (Husovec & Roche Laguna, 2022, pp. 4–5). The specific obligations for Very Large Search Engines will not be covered. Due to the focus of this thesis on VLOPs and the specific obligations linked to them, only a brief overview of all the obligations will be given, underlining, that not all aspects and legal debates around obligations can be covered. This will be followed by a more detailed outline of the specific obligations of VLOPs.

Table 1 *Due diligence obligations in the Digital Service Act*

The Digital Service Act (Chapter III)	Type of service	Due diligence obligations
Section 1	All intermediary services, including hosting services, online platforms, VLOPs	Points of contact or legal representative Terms and conditions Transparency reporting

Section 2	Hosting services, including online platforms and VLOPs	Notice and action mechanisms: Obligation to provide information to users, obligation to notify authorities in case of serious crimes
Sections 3 & 4	Online Platforms including VLOPs	Internal complaint system Out-of-court dispute settlement Trusted flaggers Measures and protection against misuse Advanced transparency report Online interface design and organisation Advertising Recommendation systems (transparency), Fair design Protection of minors Right to inform: consumer notification and marketplace transparency
Section 5	VLOPs	Risk management obligations: Risk assessment, Mitigation of risks, Crisis response mechanism, independent auditing Specific obligations on recommendation systems and advertising Data access and security: Data sharing with authorities and researchers Compliance function Specific transparency reporting obligations

Source: own illustration based on the DSA chapter III (European Union, 2022, pp. 48–78) and (Husovec & Roche Laguna, 2022, p. 5; Turillazzi et al., 2023, p. 87).

The obligations that the DSA impose are defined in Chapter III and structured into sections. Section 1 covers the obligations for all intermediary services. Section 2 covers hosting services, including online platforms and VLOPs. Sections 3 and 4 cover obligations for online platforms and VLOPs. And section 5 covers obligations for VLOPs (European Union, 2022).

Intermediary services must implement a single point of contact for authorities and users. Furthermore, the services are obligated to explain in their terms and conditions, whether and how they moderate third-party content on their services. The content moderation practices must be described, illuminating if and how they use automation. This is linked to the transparency obligations, in which the services must publish annual reports (transparency reports) explaining their content moderation practices. The DSA underlines that it must explain how automation is used in content moderation (e.g. what tools are used, for what purpose, accuracy and how mistakes are avoided) (Husovec & Roche Laguna, 2022, pp. 5–6). The information must be made public, in a way that they are easy to understand and accessible (Kalbhenn, 2021, p. 56).

Those obligations go along with obligations for **hosting services, online platforms and VLOPs**.

Those providers must implement mechanisms that allow individuals or entities to notify them in the case of illegal content (Chiarella, 2022, p. 45).

Illegal content is defined by the DSA in Article 3 (h) as the following: “*‘illegal content’ means any information that, in itself or in relation to an activity, including the sale of products or the provision of services, is not in compliance with Union law or the law of any Member State which is in compliance with Union law, irrespective of the precise subject matter or nature of that law.*” (European Union, 2022, p. 42).

Therefore, information that itself could be illegal (e.g. hate speech, terrorist content, unlawful discriminatory content) and illegal activities (e.g. content showing sexual abuse of children, cyber-stalking, sale of illegal products) are covered by this definition of illegal content (Buiten, 2021, p. 366). This is a very broad definition of illegal content, which makes the scope of application for the DSA very wide. Particularly the inclusion of “activities”, leads to a wide scope of application (Kalbhenn, 2021, pp. 52–53). It must be underlined, that mandatory removal is only applicable in the context of illegal content. Harmful but not illegal content, like disinformation, is not defined in the DSA (Buiten, 2021, p. 366).

In that regard hosting services have to provide their users with detailed information if a restriction is imposed on their content (Chiarella, 2022, pp. 45–46). If the services have information and become aware of content that could be a serious crime or lead to one, authorities must be notified (article 18 no.1) (European Union, 2022, p. 52). Particularly in the case of online platforms, this aspect is relevant. Due to the importance of platforms for the distribution of information to the public, they are faced with the role of deciding what harmful content is and when to remove it. In the context of public and political debates, this underlines how much power platforms have, for example, they were able to suspend the US president, Donald Trump’s Facebook and Twitter (now X) accounts, which shows that platforms are in a powerful position (Buiten, 2021, p. 362).

The notification obligations named by the DSA only apply to the case of illegal content, which means that the violations of terms and conditions are left unregulated by the DSA and thus are still subject to the services themselves (Husovec & Roche Laguna, 2022, p. 6). Furthermore, the reappearance of illegal content is not regulated by the DSA. There is no obligation for the services to ensure, that the illegal content, which was removed does not appear again on the platforms (Buiten, 2021, p. 374).

This is followed by the obligations for **online platforms and VLOPs**, except micro and small enterprises, which are excluded from the obligations, even though they could fall into this category (Chiarella, 2022, p. 46).

Article 22 entails that online platforms and VLOPs are obligated to integrate so-called “Trusted Flaggers”, which have expertise in identifying and detecting illegal content (European Union, 2022, p. 56). The member states can grant the trusted flaggers status to for example NGOs or other organisations that have expertise. Their notifications will be prioritised in the notification system and thus processed faster (Buiten, 2021, p. 375). Linked to this an internal complaining mechanism must be integrated, which allows users to notify the platforms in case of content that needs to be investigated (Husovec & Roche Laguna, 2022, p. 7). These complaint mechanisms should enable users who are affected by restrictions, such as the removal of content due to classification as illegal, to be lodged against the decision taken by the platform service. Furthermore, an out-of-court dispute settlement has to be integrated (Chiarella, 2022, p. 46). This approach underlines that the DSA seeks to ensure control over **how** content is removed (Buiten, 2021, p. 379).

Advertisement has to be labelled and explained, including an explanation based on which parameters the advertisement is shown and on whose behalf the advertisement is shown (European Union, 2022, p. 59). The DSA highlights how advertising on targeting techniques can have serious negative effects, especially when the targeting is based on profiling. Societal harm can arise out of the categories that are used for profiling, due to potential discrimination, disinformation campaigns or manipulative potential. That is why online platforms should not use profiling, based on personal data (European Union, 2022, p. 18). In article 26 no.3 the DSA specifies that online platforms should not use profiling in the context of special categories of personal data (European Union, 2022, p. 59). The special categories referred to can be found in the General Data Protection Regulation article 9 no. 1 *“Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.”* (European Union, 2016, p. 38).

In that regard “dark patterns”, which are veiled practices, that take place mostly on the interface of online platforms, tarnishing users’ choices and decision-making, are prohibited. In article 25 it is specified, that it is not allowed to influence the interface of the platforms in a way, which

affects the ability of users to make autonomous and informed choices or decisions (European Union, 2022, p. 18).

The parameters of the recommendation systems (timelines, recommended videos etc.) need to be explained in the terms and conditions of the online platforms. To ensure the information a transparency report must be published twice a year, including the number of monthly users (Husovec & Roche Laguna, 2022, pp. 8–9; Kalbhenn, 2021, p. 57). Recommendation systems are defined in article 3 (s) as *“fully or partially automated system used by an online platform to suggest in its online interface specific information to recipients of the service or prioritise that information [...]”* (European Union, 2022, p. 43).

With this transparency approach, the DSA tries to tackle disinformation and harmful content, instead of removing it, which could intervene with fundamental rights, such as the right to expression and free speech (Buiten, 2021, pp. 366–367).

Moreover, if online platforms permit minors access to their services based on their terms and conditions, or the services are directed at minors, or the online platform is aware that minors use the platform they are responsible for ensuring privacy, safety and security for minors using their services (European Union, 2022, p. 19).

Finally, the obligations that **only VLOPs** must comply with will be outlined in detail. The DSA specifies the reasons for those specific obligations only for VLOPs, by underlining what a critical role they play in locating and making information retrievable online (Recital 75). This critical role results from the size and reach of digital services. They play an important role in facilitating public debates, economic transactions, and the dissemination of information. Thus, VLOPs have the power to influence the distribution of information, opinions and ideas, which poses specific risks to society that smaller online platforms may not pose. Therefore, specific obligations for VLOPs are needed (European Union, 2022, p. 21).

Article 34 no. 1 specifies that VLOPs must *“diligently identify, analyse and assess any systemic risks in the Union stemming from the design or functioning of their service and its related systems, including algorithmic systems, or from the use made of their services.”* (European Union, 2022, p. 64).

Risks-based approaches have emerged historically out of social transformations and are a reaction to how modern society, tries to govern and manage risks that are created by transformation processes (Alemanno, 2016, p. 192). Especially technology poses challenges for governments in the context of regulation, due to its flexible and rapidly changing nature. In this

regard, the European Union is faced with the challenge of regulating mostly private businesses, which are the driving force of innovation and technology (Gregorio & Dunn, 2022, p. 1).

This can be linked back to the “risk society”, which was outlined in the previous chapter. The role of governments in a risk society is linked to the protection of society from risks (Alemanno, Butter, Nijssen, & Torriti, 2016, p. 1). The definitions of risks as already shown can vary because there is no universal definition. Risk regulation can be seen as an attempt by governments to face the challenges of the risk society. The assessment of modern challenges are mostly practices based on risk management, in which methods and tools should enable a rational understanding of potential threats on which decisions are based. It is important to highlight, that risk as a parameter can be employed in diverse ways within regulations, depending on the goal of the regulators, which is mostly to reduce risks to an acceptable level. The European Union has used risk-based approaches as the way forward to deal with technological developments, which is particularly evident in the case of the Digital Service Act. This regulation can be seen as an attempt to increase the accountability and responsibility of private actors, through a risk-based approach (Gregorio & Dunn, 2022, pp. 2–3).

In the DSA (Article 34 no. 1) the following **systematic risks** have been identified:

“(a) the dissemination of illegal content through their services;

(b) any actual or foreseeable negative effects for the exercise of fundamental rights, in particular the fundamental rights to human dignity [...], to respect for private and family life [...], to the protection of personal data [...], to freedom of expression and information, including the freedom and pluralism of the media, [...], to non-discrimination [...], to respect for the rights of the child [...] and to a high-level of consumer protection [...];

(c) any actual or foreseeable negative effects on civic discourse and electoral processes, and public security;

(d) any actual or foreseeable negative effects in relation to gender-based violence, the protection of public health and minors and serious negative consequences to the person’s physical and mental well-being.” (European Union, 2022, p. 64).

In the DSA it is specified, that VLOPs should assess whether and how the systematic risks that have been identified are influenced by intentional manipulation of the services such as automated exploitation (European Union, 2022, p. 64).

Systematic risks can be referred to as “[...] *the risk or probability of breakdowns in an entire system, as opposed to breakdowns in individual parts or components, and is evidenced by co-movements (correlation) among most or all parts.*” (Kaufman & Scott, 2003, p. 371).

The DSA does not give any information on how a risk assessment should be conducted by the platforms and thus does not define an approach on how businesses should identify specific systematic risks on their platforms (Loi, 2023, pp. 2–3). According to Peukert (2021), this is of particular relevance, because the DSA leaves important decisions up to the VLOPs (Peukert, 2021, p. 23).

More information is given on **factors that may influence systematic risk** and should be taken into consideration for the risk assessment (article 34 no. 2):

- “(a) the design of their recommender systems and any other relevant algorithmic system;*
- (b) their content moderation systems;*
- (c) the applicable terms and conditions and their enforcement;*
- (d) systems for selecting and presenting advertisements;*
- (e) data-related practices of the provider.”* (European Union, 2022, p. 64).

It can be concluded, that the specific obligations for VLOPs are mainly based on a risk assessment which focuses on outlining systematic risk (European Union, 2022, p. 64). With the risk assessment, the DSA moves towards an *ex-ante* approach (Turillazzi et al., 2023, p. 98). This risk-based approach is heavily employed by the EU in the context of digitalisation. That is the case because the EU is trying to balance the protection of fundamental rights, whilst fostering technological innovations for the economy at the same time. Thus, the goal of the DSA is not to minimise risks to the fullest but rather to use a “mature” risk assessment, which enables more control over the risks (Gregorio & Dunn, 2022, pp. 4–5).

Risk-based regulations can be defined as the following: “*as a set of detailed rules about which risks to accept and what measures need to be taken to minimise those risks.*” (Alemanno, 2016, p. 197). This definition underlines that the risks are not only the object of the regulation but also the justification for the regulation (Alemanno, 2016, p. 197).

To assess compliance with the due diligence obligations VLOPs must submit their risk reports to independent auditors as defined in Article 37. The reports will be submitted to the EU Commission and made available redacted to the public (Husovec & Roche Laguna, 2022, p. 10).

In this respect, it must be underlined, that the outsourcing of the application and enforcement of the regulation to private entities, such as third-party auditors, who monitor the compliance with the DSA is problematic and must be seen critically (Cauffmann & Goanta, 2021, p. 768). Private auditors are competition and profit-based, which makes it questionable and unclear whether or not the audit firms are operating independently from the online platform. Hence, the auditors of VLOPs also need to be audited, to ensure a sufficient compliance with the DSA (Cauffmann & Goanta, 2021, p. 771).

Apart from this VLOPs must implement a crisis response mechanism, in case of a serious threat to the public. Through this mechanism, the Commission can ask VLOPs to implement certain actions (Chiarella, 2022, p. 48). The DSA enforcement mechanism involves diverse actors, nevertheless, the Commission has direct supervision powers over VLOPs (Vergnolle, 2021, p. 106).

Continuing with the specific obligations for VLOPs in Article 38, they must offer their users at least one option, in which their recommendation system is not based on profiling (European Union, 2022, p. 69). In that context it is important to underline, that this option has not to be set up as a default, meaning, that users have to actively choose this option and change it in their settings (Husovec & Roche Laguna, 2022, p. 10).

Additional transparency on online advertisement is postulated by VLOPs. They must integrate a “repository”, containing information on their advertisement practises, which needs to be available to the public. The information in the repository should include detailed information, such as information on who paid for the advertisement, to whom it was presented and the period in which the advertisement was presented (Article 39 no. 1 and no. 2) (European Union, 2022, p. 69). This is an important aspect, as the algorithmic transparency strategy is one of the most crucial elements of the DSA (Chiarella, 2022, p. 52). Moreover, VLOPs must explain in their transparency reports what human resources they use for content moderation (Husovec & Roche Laguna, 2022, p. 10).

This is linked to the transparency-driven approach of the DSA, which needs to be seen critically (Rodríguez de las Heras Ballell, 2021, p. 83). That is the case, because this approach does not address targeted online manipulation based on technology sufficiently, due to its focus on giving information about procedures, rather than targeting the data collection processes and the monitoring of users in a more concrete manner (Turillazzi et al., 2023, p. 96).

Moreover, VLOPs must share data with authorities and researchers (Turillazzi et al., 2023, p. 87). The Commission should have access to all data necessary to monitor and assess the

compliance of the services within the DSA. Furthermore, researchers, that the Digital Service Coordinator has granted a status to, should have access to data enabling to conduct research related to the detection and understanding of systematic risks (Husovec & Roche Laguna, 2022, p. 10).

Finally, VLOPs must appoint a compliance officer, who is responsible for monitoring compliance with the DSA (Chiarella, 2022, p. 48).

4.2.3 Mitigation Measures

The European Commission has identified mitigation measures in the DSA, based on the identified systematic risks and the factors that might influence systematic risks. Those mitigation measures are relevant in the context of this thesis, which is why in the following the mitigation measures will be outlined. The DSA presents in Article 35 no. 1 a list of mitigation measures, that includes the following:

“(a) adapting the design, features or functioning of their services, including their online interfaces;

(b) adapting their terms and conditions and their enforcement;

(c) adapting content moderation processes, including the speed and quality of processing notices related to specific types of illegal content and, where appropriate, the expeditious removal of, or the disabling of access to, the content notified, in particular in respect of illegal hate speech or cyber violence, as well as adapting any relevant decision-making processes and dedicated resources for content moderation;

(d) testing and adapting their algorithmic systems, including their recommender systems;

(e) adapting their advertising systems and adopting targeted measures aimed at limiting or adjusting the presentation of advertisements in association with the service they provide;

(f) reinforcing the internal processes, resources, testing, documentation, or supervision of any of their activities in particular as regards detection of systemic risk;

(g) initiating or adjusting cooperation with trusted flaggers [...] and the implementation of the decisions of out-of-court dispute settlement bodies [...];

(h) initiating or adjusting cooperation with other providers of online platforms or of online search engines through the codes of conduct and the crisis protocols [...];

(i) taking awareness-raising measures and adapting their online interface in order to give recipients of the service more information;

(j) taking targeted measures to protect the rights of the child, including age verification and parental control tools, tools aimed at helping minors signal abuse or obtain support, as appropriate;

(k) ensuring that an item of information, whether it constitutes a generated or manipulated image, audio or video that appreciably resembles existing persons, objects, places or other entities or events and falsely appears to a person to be authentic or truthful is distinguishable through prominent markings when presented on their online interfaces, and, in addition, providing an easy to use functionality which enables recipients of the service to indicate such information.” (European Union, 2022, p. 65).

The mitigation measures underline the different stages of risk-based regulation that the DSA proposes. In the first step, digital services are categorised into different types of services. Those categories are linked to different systematic risks and mitigation measures. In the second stage, the online services must act upon the obligations and mitigation measures listed above (Gregorio & Dunn, 2022, p. 21).

Given this, it must be underlined, that many aspects of the mitigation measures are unclear and would need a more detailed explanation. The provisions are very vague and leave a wide room for interpretation (Barata, 2021, p. 3). To give an example the out-of-court dispute settlement could lead to the dispute resolution being dominated by private businesses, due to their powerful position compared to its users. In that, the DSA does not give concrete information on how to deal with problems linked to this aspect (Cauffmann & Goanta, 2021, p. 770). Furthermore, the DSA does not define the form of removal obligations, which leaves a wide leeway for interpretation and action open (Peukert, 2021, p. 24).

In that regard, it is important to highlight, that the involvement of civil society organisations is only mentioned in the context of developing a risk assessment and the codes of conduct, but is not part of the mitigation measures (Cauffmann & Goanta, 2021, p. 768).

4.2.4 Liability

The liability of digital services is deeply interwoven with due diligence obligations for the platforms, concerning mainly the process and design, instead of the content itself. The due diligence obligations mean that the platforms are not liable for their users, but are accountable for their failing to comply with the obligations of the DSA (Husovec & Roche Laguna, 2022,

p. 1). Due to the complex nature of legal debates around liability, only the liability of online platforms will be outlined.

Under the e-commerce directive platforms had no obligation to monitor content on their services, which led to platforms not being liable if they had no knowledge about illegal activities or acted immediately after getting notified. This principle was adopted in the DSA, in which there is no monitoring obligation. Instead, it is highlighted, that there is no general obligation to actively review content on the platforms (Heldt, 2022, pp. 70–72). Instead, the DSA seeks to create incentives to be active players against illegal content, without the risk of becoming liable (Buiten, 2021, p. 373).

As already mentioned, online platforms are included in the category of hosting services. These services benefit from a liability exemption. Online platforms are not liable for the information stored if they have no knowledge about any illegal activity or content linked to the information or have knowledge about the illegal content and take immediate actions to remove or disable access to the content (Cauffmann & Goanta, 2021, p. 764). Online platforms are not liable if they remain passive or get notified and act accordingly to the obligations linked to the notification. That is why the focus is not on liability, but rather on responsibility, which grows simultaneously as the platforms grow in size and societal impact (Husovec & Roche Laguna, 2022, pp. 3–4).

The DSA only highlights the liability exemptions for online platforms but does not give any information under which conditions a liability for online platforms would be given, which leaves it up to the member states (Turillazzi et al., 2023, pp. 101–102).

The liability aspect is problematic because it may encourage platforms to monitor their content passively to escape liability. Moreover, the fact that the DSA includes a mechanism in which users can notify the platforms about illegal content, may encourage online platforms to rather remove more than less content (Turillazzi et al., 2023, p. 95).

Especially in the case of automated monitoring, concerns are linked to an over-removal of content and thus a form of censorship, which curtails fundamental rights, such as freedom of expression and speech (Rodríguez de las Heras Ballell, 2021, p. 84). Thus, the DSA faces a dilemma between protecting citizens and users of online platforms through the regulation, whilst at the same time ensuring fundamental rights, such as freedom of expression and data protection. Given this, it is still unclear if the DSA addresses fundamental rights correctly (Turillazzi et al., 2023, p. 91).

Thus, the DSA is faced with the complex task of balancing different rights for different stakeholders. Fundamental rights of expression and freedom must be protected, as well as rights to privacy for users of online services, whilst respecting the platform's rights to conduct business (Frosio & Geiger, 2020, pp. 13–14). Further research needs to be done in the future to investigate the DSA and online platforms and their impact and fundamental rights.

Finally, it must be mentioned, that in the case of VLOPs, the Commission will have the power to demand compliance. Online platforms can be fined up to 6% of their worldwide turnover if they do not comply with the DSA (European Parliament, 2022a).

In summary, it can be seen that the Digital Service Act is a large and complex regulation, which is trying to protect fundamental rights whilst ensuring technological innovations. With the DSA significant developments in regulating online platforms based on the new due diligence obligations have been put forward (Buiten, 2021, p. 379). Nevertheless, the remarks made have illuminated that many complex challenges go along with regulating digital services. How effective the DSA will be in protecting fundamental rights sufficiently, especially in the context of private online businesses is still an open question.

5. Methodology

The outlined work on the digital risk society, the platform economy, and the Digital Service Act have highlighted, that the field of interest is very topical and seems to be only emerging. By applying an interdisciplinary approach, this thesis addresses a specific angle of research by combining perspectives from different disciplines to systematically elaborate on digital risks and draw implications from this in the context of their regulation.

In the first step, the process of conducting the literature for chapters 1-3 will be illuminated. The reason for that is that the literature review represents the base for the case study analysis and the discussion. This will be followed by a description of how the case study analysis will be executed in a way which will enable to answer the following research question:

How are digital risks, which arise from social media platforms linked to the data-driven value creation within the platform economy? And what are the implications in the context of the Digital Service Act?

As already mentioned, the first part of this thesis (Chapters 1-3) consists of a literature review. Due to the complexity and topicality of the subject, it is relevant to give an overview of the current state of the art. A literature review represents the foundation for an analysis, which can

advance knowledge and facilitate further research by illuminating research gaps (Snyder, 2019, p. 333).

Snyder (2019) has defined a literature review as *“a more or less systematic way of collecting and synthesizing previous research.”* (Snyder, 2019, p. 333).

There are diverse ways in which a literature review can be conducted. When studying a broad topic, which has been conceptualised by different disciplines in various ways an “integrative review” enables a combination of perspectives (Snyder, 2019, p. 334). The literature was conducted in a similar way to an integrative review. That is the case because the claim is not to give a full overview of all research that has been done. Rather the purpose is to carve out the new emerging research field and outline the need for further research.

An integrative review is characterised by the examination of literature by highlighting the main ideas and relationship of an issue. Because of this no strict standard is applied in an integrative review because the analysis does not follow a specific standard. Rather the purpose of the research guides the review, which enables the researcher to illuminate relevant aspects for answering the research question (Snyder, 2019, p. 336).

Thus, this thesis does not claim to give a completely systematic overview. No strict standard was applied whilst conducting the literature, rather the focus on digital risks has made it possible to thematically identify literature that can enable to grasp digital risks in the context of society and regulations. In that regard, it is important to highlight, that the newness of the topic, especially in the context of the Digital Service Act makes it impossible to apply a strict systematic method.

The purpose of the literature review is to combine perspectives and insights from different fields, to be able to understand the research field and answer the research question (Snyder, 2019, p. 336). Thus, the literature review was conducted from within diverse disciplines namely risk studies, computer science, legal studies, economics, sociology, political science, and business studies. This highlights the interdisciplinarity of the subject and this thesis.

Interdisciplinary research is characterised by the interaction of two or more disciplines (Danermark, 2019, p. 369). The conducted literature review has underlined that the field of risks, technology and society has been studied within diverse disciplines, but rarely in an interdisciplinary way.

Danermark (2019) has highlighted, that in our current world interdisciplinary research is needed, due to the global, complex and interconnected nature of current issues, which society

is facing. Academic research must go beyond disciplinary boundaries, to enable an understanding of current issues. In view of this interdisciplinary research is challenging because knowledge from different research fields must be integrated (Danermark, 2019, pp. 368–369). Therefore, the digital risk society cannot be studied from one discipline only, because the nature of the field is deeply interdisciplinary.

Concluding, this thesis does not give a holistic overview of all research done but rather systematically works out relevant aspects regarding digital risks. The conducted literature work helps to give an overview of the research from different disciplines, which is particularly important in the context of interdisciplinary research subjects (Snyder, 2019, p. 333).

Considering this the thesis needs to integrate perspectives from: (1) a sociological (2) an economic (3) a legal pillar.

The sociological pillar has focused on digital risks and society. The traditional work on the risk society has been systematically outlined and connected to the current research on the new emerging research field of the digital risk society.

The economic pillar has outlined characteristics of the platform economy focusing on the way value is generated. A focus was set on the monetisation of personal data, due to the relevance of data-driven platform businesses for the digital risk society and the Digital Service Act.

Finally, the legal pillar has outlined the Digital Service Act, which recognises that digital risks for society arise from platform businesses. The Digital Service Act focuses on regulating digital risks through risk assessment and mitigation measures, which are supposed to protect society from digital risks.

Those three pillars will be combined in the analytical part enabling a deep understanding of digital risks, society and how they are trying to get regulated by the European Union. Employing the perspective of the EU on what digital risks are and how they should be regulated provides an insight into what role platform businesses play in society and how they are deeply involved in the negotiation process regarding digital risks in the digital risk society.

A case study analysis is used for the research purpose. The analysis does not have the claim to generalise the information retrieved but rather pursues an illustrative claim. Therefore, the case studies, which were chosen are used as illustrative examples, which help to answer the research question by understanding the mechanisms of platform businesses and how this is linked to digital risks.

Yin (2018) has defined a case study as *“an empirical method that investigates a contemporary phenomenon (the “case”) in depth and within its real-world context, especially when the boundaries between phenomenon and context may not be clearly evident.”* (Yin, 2018, p. 15).

Case studies can be categorised into three types (1) explanatory (2) descriptive (3) exploratory case studies (Yin, 2018, p. 9). This thesis uses an exploratory case study, as the purpose of the analysis is to understand a field which recently emerged and thus has only been researched to a limited extent.

Exploratory case studies are grounded in a combination of literature review, research question and the development of a theoretical framework or illustration of a research gap (Ridder, 2020, p. 112). That is the case for the following analysis as the goal is to understand and highlight digital risks which are emerging from platform businesses.

In that context it must be noted, that case study research has been facing criticism in academia, due to its lack of systematic methodology and inability to generalise from case studies (Yin, 2018, pp. 19–20). Nevertheless, particularly in business studies, case study research is employed and used to understand businesses and economic processes (Widner, Woolcock, & Ortega Nieto, 2022, pp. 1–2). This is particularly relevant considering the research question and the proximity to practice by using real-world case studies.

Wider et al. (2022) have highlighted, that case studies are a particularly useful method for developing theory or identifying “causal mechanisms” especially in the context of exploring “black box” processes (Widner et al., 2022, p. 4). Moreover, Yin (2018) has underlined that case studies can contribute significantly to the expansion of knowledge by exploring real-world cases (Yin, 2018, p. 49).

Against this background case studies can answer diverse research questions (Hering & Jungmann, 2022, p. 678). Ridder (2020) has highlighted, that research questions in the context of case studies often fail to indicate the direction the research is going in, which is why a “proposition” is needed (Ridder, 2020, p. 114).

The proposition (e.g. hypothesis) for this thesis is defined as the following: Digital risks may represent a prerequisite for the platform economy because some of the systematic risks identified by the DSA are deeply intertwined with the way profit is generated by VLOPs.

Case studies can also contain multiple cases, the so-called “multiple-case studies” (Yin, 2018, p. 17). For this thesis, a multiple-case study is employed, because two social media platforms are used as cases. Against this background, the chosen case studies “TikTok” and “Instagram”

represent data-driven platform businesses, which function as illustrative examples of platform businesses.

The reasoning behind choosing multiple cases lies in the limited research done so far and the similarity of the cases, which enables a more profound illustration of the mechanisms within the platform economy.

The cases for case study analysis can be chosen in different ways and for different reasons (see Hering & Jungmann, 2022, pp. 680–681). Longhofer et al. (2017) have underlined that case studies are particularly useful if they have a strong and significant explanatory power (Longhofer et al., 2017, p. 190).

Firstly, TikTok and Instagram were chosen based on the outlines in the Digital Service Act. The specific focus on “Very Large Online Platforms” is driven by them facing the most specific obligations to comply with (Husovec & Roche Laguna, 2022, pp. 4–5). As already mentioned in Chapter 5 this role defined by the EU results in the size and reach of VLOPs. They play a critical role in society by facilitating public debates, economic transactions, and the dissemination of information. Thus, VLOPs affect the distribution of information, opinions, and ideas, which poses specific risks to society (European Union, 2022, p. 21). Against this background, the cases chosen have been qualified as VLOPs by the EU (European Commission, 2023b).

Secondly, social media platforms were chosen specifically due to their relevance to everyday life and the risks they pose to society. Noting that the characteristics of social media platforms have not been explained thus far, only a brief outline will be given, which highlights the reason for choosing social media platforms as case studies. That is the case because the definitions of social media and platforms in general overlap considerably. That is why the specific characteristics of social media will be elaborated on in the context of the case study analysis.

Gawer and Srnicek (2021) have pointed out, that the definitions of online platforms include social media (Gawer & Srnicek, 2021, p. 2). Therefore, using social media as illustrative examples can give an inside into the way the platform economy is functioning, structured and structuring.

Social media can be defined in diverse ways, nevertheless, all definitions have some similarities, which highlight the relevance for society and everyday life (see Fuchs & Kurz, 2021, pp. 57–61). Without going into detail on social media definitions, they can generally be described as internet-based network platforms, which enable communication (Meikle, 2016, p. x). Moreover, social media platforms do not only enable communication, but are also used for

sharing and consuming information and thus represent a space for public discourse (Lee, Lindsey, & Kim, 2017, p. 254). Social media platforms are data-driven business models, which particularly use personal data for their value creation (Corcos & Hodara, 2023, p. 117).

The cases TikTok and Instagram represent two social media platforms, which function similarly and are getting heavily used, which is why they were chosen as illustrative examples in this thesis.

TikTok has had approximately 125 million “monthly active recipients” in the European Union from August 2022 to January 2023 (TikTok, 2023c). Instagram had 259 million average monthly active users from April 2023 to September 2023 in the European Union (Instagram). Those numbers highlight the relevance of those two platforms, due to a high use across the EU. TikTok represents one of the leading social media platforms, which influences the developments in the social media industry, due to its unique interface and algorithmic recommendation system (Botero Arcila & Griffin, 2023, p. 75).

Instagram on the other side is part of Meta Platforms Inc. (former Facebook Inc.), which is a company that includes other platforms such as WhatsApp and Facebook in their portfolio (Madhura K. & Niyaz Panakaje, 2022, pp. 355–356). This highlights that Instagram is not only a relevant social media platform but also part of one of the biggest and most influential business companies regarding social media. That is why it is particularly interesting to use Instagram as a case study because the business logic of Instagram is representable for all platforms and products of Meta.

Given this, it is interesting to use a US company (Instagram) and a Chinese company (TikTok), as the standards on the platforms vary and the influence of Chinese platform businesses has had an effect on the developments within the platform economy (Zeng et al., 2021). Acs et al. (2021) have highlighted, that US companies and Chinese companies are in competition with each other, which is linked to power and monopoly aspects of the platform economy (Acs et al., 2021, p. 1643).

Moreover, TikTok and Instagram function in a similar way, as they are based on short video content, which has developed and dominated the social media market in recent years (Zeng et al., 2021, p. 3162).

The cases were chosen based on them representing some sort of “standard” cases (Hering & Jungmann, 2022, p. 681). Hence, the chosen cases are representative examples of the way social media platforms function in the platform economy. This can give insights into the logic of data-driven platform businesses and the platform economy. Noting that the platform

economy contains diverse business models the chosen case studies are not representative of all business models, which is why the results cannot be generalised.

Moreover, the availability of studies was an important factor to take into consideration, when choosing the cases. The reason for that is the very limited research in the context of digital risks for society. Since I have done some previous research on TikTok and Facebook during my studies in International Development and Socioeconomics I was sure that some relevant studies are available (El-Aawar, 2020, 2023). This aspect is of particular importance as this thesis is informed partly by my previous research.

It is characteristic for case study analysis, that multiple sources of evidence are needed (Yin, 2018, p. 15). As already mentioned, the relevant literature is very limited. Consequently, multiple sources are used for the analysis, as this thesis relies on secondary literature. On the one side studies and academic literature from diverse disciplines will be outlined through books and academic journals and on the other side information will be directly extracted from social media platforms. That is why the sources used for the analysis also contain business reports, studies conducted by the EU in the context of the DSA and information from the websites of the platforms, including their specific websites for developers, engineers, and businesses.

After the reasoning behind the case selection is described, the procedure of the analysis will be explained in detail.

Firstly, the case TikTok and Instagram are outlined and characterised as data-driven business models of the platform economy. A specific focus will be on how platform businesses function and what mechanisms are used to generate profit. This will be linked back to the data-driven value creation of the platform economy.

In a second step studies are outlined which have researched the aspect of digital risks on TikTok and Instagram. As already mentioned, the conducted research is thus far very limited. Different databases are used to find studies on Instagram and TikTok, such as Google Scholar, U:search (university of Vienna), Scopus, the publications office of the European Union and the DSA Transparency Database of the European Commission. In that regard, the purpose is not to give a holistic overview of all studies published, but rather to look for studies, which can be used to illustrate digital risks which arise out of the economic logic of social media platforms.

Due to the large scope of digital risks, the focus will be on the following chosen digital risks outlined in the DSA: (1) misinformation/ disinformation (2) mental/physical wellbeing (3) children/ young adults and (4) discrimination and bias.

For transparency reasons some of the used search terms (which were combined in diverse ways) will be outlined in the following: “digital risks”, “TikTok”, “Instagram”, “algorithm”, “challenges”, “threats”, “democracy”, “misinformation”, “disinformation”, “wellbeing”, “mental health”, “bias”, “discrimination”, “children”, “young adults” “algorithmic recommendation system”, “artificial intelligence”, “machine learning”, “filter bubbles” and “personalisation”.

The outlined digital risks will be analysed based on the conducted literature on the platform economy and the digital risk society. By linking the case studies with the digital risk society, the platform economy, and the Digital Service Act general information on digital risks and how they are trying to get regulated can be drawn from the illustrative examples. This will enable to answer the research question, by critically discussing the role platforms play and how the EU regulation may fail to sufficiently protect society from digital risks. Moreover, the analysis will enable an understanding of how the EU perceives digital risks and what role the EU has ascribed to platform businesses in the context of regulating digital risks.

Concluding it must be underlined that this thesis and analysis has its limitations. The platform businesses do not give any detailed information on the technology used, which is why the analysis in this thesis is confronted with the problem of becoming speculative, due to the lack of detailed information and evidence, especially in the context of the algorithmic recommendation systems, which are described as “black boxes”, due to their lack in transparency (see Pasquale, 2015).

In addition, the case studies used are only illustrative examples, which is linked to the general limitations of case study research. The lack of systematic methodology and the inability to generalise from case studies limits the results of the analysis (Yin, 2018, pp. 19–20). Due to the lack of research done thus far and the use of secondary sources, only no new empirical evidence can be drawn from this thesis. Nevertheless, this thesis draws attention to a research gap and highlights the need for further research in that field.

Furthermore, the literature and studies used for this thesis are in the languages English, German, and French. Even though the Chinese platform TikTok is being used as a case study, no literature in Chinese or any other language is used for this thesis. In that regard, the lack of language skills limits the perspective and research conducted for this thesis.

Finally, the studies used regarding mental and physical wellbeing are mainly extracted from the disciplines of psychology and medicine. Due to a lack of expertise in those disciplines, the specific and complex methods used for the studies cannot be explained or fully grasped. Rather

the selection process relies on the publications of the studies in acknowledged academic journals and the metrics of the studies (e.g. number of how often a study was cited).

The claim and purpose of the analysis is not to give a holistic overview of digital risks or to evaluate the way the EU is regulating digital risks. Rather the field of digital risks in the context of the platform economy is carved out, by illustrating the relevance of the research field and thus highlights that further research is needed. This is particularly the case in the context of the obligation for VLOPs in the DSA, as they must share data with researchers, which enables them to conduct research related to the detection and understanding of systematic risks (Husovec & Roche Laguna, 2022, p. 10; Turillazzi et al., 2023, p. 87).

6. Case Study Analysis: Digital risks as a side effect of social media businesses?

6.1 Characterising social media

In the first part of this thesis data-driven platform businesses have been outlined from a general perspective. In the following part, the specific case of “social media” as an essential part of the platform economy will be explained. The key characteristics of platform businesses, which have been explained in Chapter 4 will be extended by the specific characteristics of social media businesses. In the first step, the general definitions of social media will be outlined, which will be followed by the introduction of the two cases “TikTok” and “Instagram”. Those will be used as illustrative examples, explaining the data-driven logic, and functioning of the platform economy in more detail.

6.1.1 Overview of social media definitions

Since there is no universally agreed-upon definition social media can be defined in various ways. Fuchs (2021) has given an overview of commonly cited social media definitions in academia (see Fuchs, 2021, pp. 28–30). In the following an overview of some of those commonly cited definitions will be given, noticing that not all existing definitions can be covered. That is why the focus will be on highlighting the similarities of the definitions and how the key characteristics of social media can be linked back to the general key characteristics of platform businesses.

Burgess, Marwick and Poell (2018) have generated a definition of social media, which combines many perspectives. They define social media as “*digital platforms, services and apps built around the convergence of content sharing, public communication, and interpersonal connection.*” (J. Burgess et al., 2018, p. 1).

Most definitions focus on social media being **internet-based network platforms**, which enable **public** and **private interactions** (Meikle, 2016, p. x). Thus, social media is based on **information technology**, which represents the **infrastructure** of the platforms (J.-H. Schmidt, 2018, p. 11).

The European Union has also developed a similar definition of social media. The European Data Protection Board (2021) has defined social media as “*online platforms that enable the development of **networks** and **communities** of users, among which **information** and **content** is **shared**.*” (European Data Protection Board, 2021, p. 4).

Social media offers individuals **digital services**, which they can register for by creating **accounts** (e.g. **profiles**), enabling an **interaction** with other **users** or **content** (European Data Protection Board, 2021, p. 4). Social media platforms enable interactions in the form of **communication** and by **sharing, creating and consuming information** (Lee et al., 2017, p. 254).

Social media platforms can be characterised as so-called “advertising platforms”. Those types of platforms have built their business models around the monetisation of data. They extracted information from their user’s (personal) data to analyse the information through technology and make predictions. Based on the extracted data individual profiles are generated which enable accurate predictions about individuals, their behaviour, and their thoughts. This output is then sold as profitable “ad spaces”, which enable the platforms to monetise the data they extracted and analysed (Zuboff, 2019, pp. 65–66) The value generation of social media platforms will be explained in more detail during the case study analysis in the second part of this chapter.

Comparing the definitions of social media with the definitions of the platform in general illuminates the similarities. Reiterating the definition of platforms from Chapter 4, Poell et al. (2019) defined platforms as “*(re-) programmable **digital infrastructures** that **facilitate and shape personalised interactions among end-users** and complementors, organised through the systematic collection, algorithmic processing, monetisation, and circulation of data.*” (Poell et al., 2019, p. 3).

Social media platforms can be used as examples, which illustrate the way platform businesses operate, because their key characteristics are in line with the general key characteristics of data-driven businesses of the platform economy.

José van Dijck (2013) has underlined in her early work on social media, that the “social” aspect of social media implies that they facilitate some sort of community. Concluding that new infrastructures in the form of “an ecosystem of connective media” emerge, based on the

interconnection of platforms (Jose van Dijck, 2013, pp. 11–12). Similarly Fuchs (2021) has highlighted that social media is not just technology, but rather a “techno-social system”, which highlights that technology is used to enable human activities, facilitating knowledge production, distribution and consumption. Thus the “social” aspect of social media is enabled by the fact that technological structures are interconnected with human agency (Fuchs, 2021, p. 31).

Social media has become a key infrastructure in the context of generating and distributing information, which is linked to diverse opportunities and challenges for society (Botero Arcila & Griffin, 2023, p. 9). The use and relevance of social media platforms have grown over the past 20 years, as they have become an (indispensable) part of individuals' everyday lives (Fuchs, 2021, pp. 40–41). Moreover, the relevance and effects on democracy have been shown by events such as the influence on the 2016 presidential elections in the United States or the spread of misinformation during the Covid-19 pandemic. This underlines, that social media is not only used for entertainment purposes and private communication but also in the context of news consumption and public discourse. Social media are digital services, which are informing the public based on the information that is spread and consumed by diverse actors on the platforms (e.g. users, advertisers, bots, etc.) (Gabarron, Oyeyemi, & Wynn, 2021; Himelein-Wachowiak et al., 2021; Lee et al., 2017, p. 254).

In conclusion, the outlined aspects of social media illuminate why the research on those platforms is of particular importance in the context of digital risks and the DSA. In the following, the two chosen case studies TikTok and Instagram will be briefly introduced. This will be extended by an outline of the function of the two platforms and how they generate profit.

6.1.2 TikTok

In 2016 the popular video-sharing app “Douyin” was launched by the Chinese company “ByteDance”. Douyin is a short video app, which gained immense popularity, because of its focus on short music and dance videos (Lu & Lu, 2019, pp. 233–234). During that time the Chinese social media market had been influenced by the rise of short-video applications (Wang & Wu, 2021, p. 3270). Because of this Douyin joined the market at a late point, because 10 short-video apps were already competing in the Chinese social media market (Zeng et al., 2021, p. 3162). Despite the high amount of competition Douyin rapidly became very popular, due to their unique editing functions, which allowed users to easily create short videos with add-ons, stickers, visual effects, animations and music (Lu & Lu, 2019, p. 234). The popularity of Douyin led to Bytedance expanding internationally, by launching TikTok in 2017 as the international version of Douyin. During that time the short video platform “Musical.ly” was

very popular among teenagers in the United States and the United Kingdom. Musical.ly was a short video app launched in 2014, which had its headquarters in Shanghai. Shortly after the launch of TikTok in 2017, ByteDance bought Musical.ly and merged the two platforms in 2018, keeping the name TikTok. During this time TikTok has rapidly gained a large user base because the users of Musical.ly had to migrate to TikTok. Moreover, the Covid-19 pandemic had a positive effect on the app, because the user base grew immensely during the pandemic (Boffone, 2022, p. 2; Zeng et al., 2021, pp. 3162–3163).

TikTok had over three billion downloads and around one billion active users worldwide (Boffone, 2022, p. 2). As already mentioned, TikTok had to publish the “number of active recipients” in the EU as an obligation of the Digital Service Act (European Commission, 2023c). Based on their published numbers TikTok has had approximately 125 million “monthly active recipients” in the European Union from August 2022 to January 2023 (TikTok, 2023c).

The popularity of TikTok has influenced other platforms, which had to adjust their design and business strategy to the new way the social media market was developing, due to the dominance of TikTok (Botero Arcila & Griffin, 2023, p. 75). TikTok dominates the teen and pre-teen market, with its users being part of Generation Z (born between 1997 and 2012) (Boffone, 2022, p. 2). That is the case because the business model of TikTok specifically targets teenagers and preteens (Zeng et al., 2021, p. 3162).

The app consists of short videos, which are 3-60 seconds long and presented on the so-called “For You Page” (Boffone, 2022, p. 2). As already highlighted TikTok stands out as a short video app because the app allows its users to easily create short videos, without needing complex editing tools or specific knowledge. Through the accessible way of integrating music, filters and special effects TikTok has become a “hub for creativity” (Zeng et al., 2021, p. 3163).

6.1.3 Instagram

Instagram was founded in 2010 in the United States as a photo-app, which enables its users to edit and share photos and images on individual profiles. The platform was one of the first applications, which allowed its users to caption images with a title and enabled other users to comment on the posted content. During Instagram’s early days, the social media app was centred around photos/images and interactions with other users (Ponnusamy, Iranmanesh, Foroughi, & Hyun, 2020, p. 2).

In view of Instagram has stood out, due to its unique features at the time. Users were able to link keywords or themes through “hashtags” with the pictures/images they wanted to upload, enabling their users to search for specific images and themes (Mattern, 2017, pp. 4–10).

In 2013 Instagram introduced short videos to the platform (Mattern, 2017, p. 4). Since then the app has not only centred around pictures and images but also around so-called “reels”, which are short videos and live stories (Ponnusamy et al., 2020, p. 2).

Due to the popularity and importance of advertising the app was bought by Facebook in 2012, but still functions as an individual platform (Ponnusamy et al., 2020, p. 2). The company Facebook Inc. (since 2021 Meta Platforms Inc, in short Meta), originally consisted of the social media platform Facebook and extended its scope by acquiring other platforms. Today Meta includes Facebook, Facebook Messenger, Instagram, WhatsApp and Oculus (virtual and augmented reality software/hardware) (Madhura K. & Niyaz Panakaje, 2022, pp. 355–356). Meta has a standardised and uniform Data Policy for all their platforms and products, which is why the platforms that are part of Meta underly the same business logic (Meta, 2023a).

Instagram has more than 1 billion monthly users worldwide and represents one of the most popular social media platforms among young adults, with its users being approximately between 18 and 29 years old (Ponnusamy et al., 2020, p. 1). Instagram had 259 million average monthly active users from April 2023 to September 2023 in the European Union (Instagram).

After the introduction of the two social media platforms the following section outlines the economic logic behind the platforms.

6.1.4 The economic logic of TikTok and Instagram

Instagram and TikTok have similar features and employ a similar economic logic. The chosen case studies, are not analysed individually, but rather considered together. Firstly, the data collection of TikTok and Instagram will be outlined, highlighting the type of data and the ways data is collected by the platforms. This will be extended by explaining the technology used for the data collection. Secondly, the monetisation of data will be outlined, focusing on how the platforms facilitate this process by using technology. Given this, the economic logic of TikTok and Instagram is illustrated based on the insights gained from Chapter 4 “The Platform Economy”.

As already explained the platform economy is characterised by data-driven business models. Profit is generated through the monetisation of data. Data-driven business models collect, extract and analyse data as a key resource (Srnicsek, 2017, pp. 254–255). Against this

background, individuals must agree to the “terms and conditions” of the platforms to be able to use the services. This agreement grants the platforms legal access to the data of its users (Rodríguez de las Heras Ballell, 2021, p. 82).

Because of this, the question arises of what type of data the social media platforms collect and how they generate profit out of it.

Firstly, it must be underlined that the conducted research has revealed, that TikTok and Instagram collect the same type of data and use it similarly (see Instagram, 2022; TikTok, 2023g). That is why the information is not outlined for each platform individually, rather the focus will be on TikTok, which will be extended by information from Instagram. The reason for that is to allow a better reading flow.

The retrieved information is directly extracted from TikTok’s “Privacy Policy”, effective since the 19th of November 2023 (TikTok, 2023g). In that regard, it must be underlined, that the detailed explanations of TikTok are summarised as much as possible, but remain very close to the original, due to the specific legal and technical language used.

TikTok states that “[...] *the TikTok app is not unique in the amount of information it collects. In line with industry practices, we collect information that users choose to provide to us and information that helps the app function, operate securely, and improve people's experience.*” (TikTok, 2023i).

This aspect is of particular interest in the context of the research question, because TikTok underlines that the way they collect data and extract information is in line with the industry's practice and legitimate, because of the consent of users and the purpose of the collection.

TikTok collects personal data, as well as technical information about its users in three ways (1) information which users provide (2) automatically collected information (3) information from other sources (TikTok, 2023g)

(1) The information, which users provide is **profile information** (date of birth, username, email address, telephone number, password, profile photo), **user content** (uploaded content such as photos, images, videos, audio recordings, live streams, comments, hashtags) and **metadata** (information on when, where and by whom the content was created). The information from user content is collected, irrespectable if they have been uploaded or not. Moreover, information is extracted from **direct messages**, shared **contacts** (if the user chooses to synchronise the contacts with the app) and **purchase information**, if a purchase or a payment is made through the platform (TikTok, 2023g).

(2) Automatically collected information includes **technical information** (device and network, IP address and system language), **location information** and **usage information** (information about the content that is viewed, the duration, frequency of use, engagement with other users, search history, settings and keystroke patterns/rhythms) (TikTok, 2023g). Moreover, **content characteristics** and **features** are collected. This is done by identifying “objects, scenery, location, faces, body parts and the text of spoken words.” (TikTok, 2023g). Moreover, **users' attributes** (e.g. age and gender) and **interests** are **inferred by TikTok** based on the information conducted (TikTok, 2023g). Moreover, TikTok collects **biometrical information**, through collecting and using **face and voice information**, which enables analytics, such as demographic classifications (TikTok, 2023i).

TikTok also has access to information from the camera and microphone, if the access is permitted by the user (TikTok, 2023i). Because of this access to the camera and the microphone must be granted to use the app, otherwise the functions will be significantly affected. TikTok does not give any information on when the platform stops to collect information from the camera and microphone. TikTok has been accused of collecting information without its user's knowledge. Particularly in the context of social media applications, it is unclear when the access to the microphone and camera ends, as users are “logged in” constantly and only close the app, which sometimes still runs in the background collecting information whilst the app is not used “actively” (Jin Kang, 2022, pp. 123–126).

(3) Information from other sources is collected through diverse other sources. For example, **third parties** (advertisers) share information with TikTok about actions that did take place outside of TikTok, such as information on purchased products. This information is used to match the actions outside of the platform with the TikTok account (TikTok, 2023g). Moreover, TikTok collects information if a user is mentioned or included in another user's content or direct messages (TikTok, 2023g). TikTok also has access to information from other apps, that are running at the same time as TikTok, including banking apps (Jin Kang, 2022, p. 125). Finally, TikTok collects information by tracking **keystroke patterns** or **rhythms** on third-party websites. TikTok underlines that they only track “that a keystroke happened on a third party website, but not which keys were pressed” (TikTok, 2023i).

As previously noted, the comparison of the Data Policy of Instagram (2022) and the Privacy Policy of TikTok (2023g) has revealed that Instagram and TikTok collect the same type of data. That is why the type of data Instagram collects will be briefly outlined, highlighting the similarities.

Instagram states, that their Data Policy covers all products of Meta, which is why Instagram is representative of how Meta collects, uses and shares data (Instagram, 2022). Meta has updated their Data Policy, which is valid from the 12th of January 2024 (Meta, 2023a).

Instagram collects data from **information and content** that the user provides (personal information, metadata, uploaded images/videos, interests from viewed content), **networks and connections** (hashtags, following pages, interactions with users and products), **usage** (type of viewed content, duration, usage time, clicks), **third party information** and **device information** (IP address, language) (Instagram, 2022).

In summary, the outlined type of data collected and used by TikTok and Instagram can be classified as mainly personal data about its users. This highlights that social media platforms are data-driven business models which generate profit from analysing and using personal data (Wessels et al., 2019, p. 13).

Against this background, it is important to highlight that both TikTok and Instagram refer to the data they collect as “information”, even though the data does not equal information. This aspect is striking in the context of the research question because it underlines the way platforms are presenting their business with data. By stating that information is collected, instead of stating that data is collected and processed into information, it seems as if the personal information exists as a “natural” resource. This aspect undermines the fact that platform businesses actively extract personal information by using technology, which is specifically developed for that purpose.

Linking this back to the definitions and discussions around the term “data” it seems like platforms are presenting personal information as a natural resource, which is freely available instead of manufactured (Sadowski, 2019, p. 2).

Huhtala (2019) has underlined, that value does not arise from the data itself, but from the retrieved information that is generated after processing the data (Huhtala, 2019, p. 56). That is why in the following it will be outlined how data is extracted by TikTok and Instagram using different types of technology, underlining that it is not as evident as the platforms make it seem to access personal data. In that regard, it must be noticed that the technology used for data extraction is very complex and only a few pieces of information are provided by the platforms. Thus, only a brief outline of a few used technologies will be given.

Meta states, that they “[...] use *cookies and similar technologies, including data that we store on your web browser* [...] and the Meta *Pixel*. They help us provide, protect and improve our Products, such as by *personalizing content, tailoring and measuring ads and providing a safer*

*experience. We collect information from **cookies stored on your device**, including cookie IDs and settings.*” (Meta, 2023c).

Cookies can be defined as *“small pieces of text used to store information on web browsers.”* (Meta, 2023c). TikTok highlights, that *“cookies can remain on your computer or mobile device for different periods of time.”* (TikTok, 2022b).

A distinction can be made between two different types of cookies (1) session cookies, which are only active when the app is used and deleted after the app is closed (2) persistent cookies, which “survive” after the app is closed. The second type of cookie can track and identify the user by assigning a unique number directly to the used device (TikTok, 2022b). Cookies can be managed by the users in the settings of the apps. When users visit the platform, they must agree to the use of cookies (all cookies allowed, or only necessary cookies allowed). The settings on cookies and other tracking technologies can be managed to an extent by only allowing “necessary” cookies (TikTok, 2022b).

Moreover, so-called “pixels” are used to extract data, which can be defined as *“small 1 pixel x 1 pixel **invisible image files** that are embedded in certain website pages.”* (TikTok, 2020). Pixels are used to collect information about the user's visits to webpages and can give information on activities, such as the opening of an email (TikTok, 2020).

Finally, “Software Development Kits” (SDKs) are used, which are *“pieces of code that enable data to be collected about your device, network and interaction with a website.”* (TikTok, 2022b)

The highlighted tracking technologies used, underline the complexity of the data collection process and the hidden way of tracking individuals and extracting personal data, which is often veiled to the users as the pixels and cookies are not visible. This aspect is of particular importance in the context of the research question, as it is often unclear what concrete information the social media platforms possess and it is used. In the following the way personal data is used by TikTok and Instagram for profit will be outlined.

As previously mentioned, Sadowski (2019) has characterised key ways, in which data generates value and is thus used by platform businesses. The analysis thus far has revealed, that TikTok and Instagram are using the data for (1) profiling and targeting individuals (2) optimising their systems (Sadowski, 2019, p. 5-6).

TikTok states *“[...] we use your information to **improve, support and administer the Platform**, to **allow** you to use its **functionalities**, and to **fulfill and enforce our Terms of Service**. We may*

also use your information to, among other things, **personalise content** you see on the Platform, promote the Platform, and **customize your ad experience**.” (TikTok, 2023g)

Also, on Instagram’s Privacy Centre, which is operated by Meta, a similar explanation of how data is used is given, namely to “provide, personalise and improve” the products (Meta, 2023a). Moreover, Meta highlights that they use the collected information to **improve their products** and **prevent harmful behaviour** on Instagram to keep its users safe (Meta, 2023a).

TikTok and Instagram function in a similar way. Individuals must register to create an account, enabling the users to access the platform services. After creating an account, users can access the main page (Instagram: Feed/ TikTok: For You Page) and other functioning’s of the of the platform (Wang & Wu, 2021, p. 3274).

The main page on TikTok is called the “For You Page” (see **Figure 2**)². The For You Page only shows short videos, as TikTok is centred around short videos (TikTok, 2023d). Also, the For You Page consists of personalised content, which is recommended by TikTok to its users (TikTok, 2023a).

In the case of Instagram, the so-called “Feed” represents the main page of the platform (see **Figure 3**). The Feed is the place where photos and videos appear when opening the app. Instagram curates the content shown in the feed, based on the information retrieved from analysing the collected data. The Feed contains content, that Instagram defines as the most relevant content for each user (Instagram, 2023a).

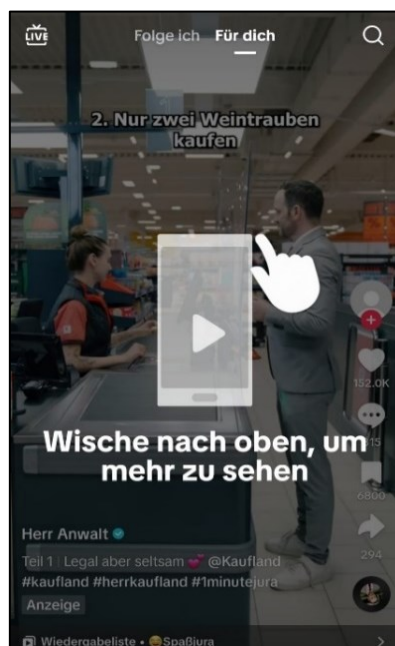


Figure 2 TikTok For You Page (TikTok, 2023d).

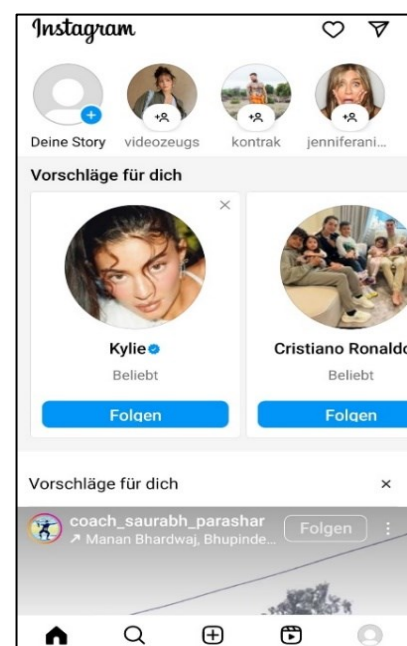


Figure 3 Instagram Feed (Instagram, 2023b).

² Figures 2 and 3 are screenshots taken directly from the applications. The device which was used for the screenshots is located in Austria, which is why the Figures contain German language.

The personalisation is based on the analysed collected data outlined above. Concerning personalisation, Instagram states that it uses the extracted personal information about its users to show personalised features and content, such as stories, ads and recommendations on its Instagram feed (Meta, 2023a).

In that context, it must be highlighted that TikTok and Instagram do not give any detailed information on how exactly they analyse the collected data. Rather, TikTok underlines, that they use the collected data to “*infer additional information about you, such as your age range, gender, and interests.*” (TikTok, 2023g).

This shows that the analytical process enables TikTok to generate additional information based on the collected data, which cannot be directly extracted from the data, but is rather inferred based on predictive analytics, using algorithms, artificial intelligence and machine learning to analyse the collected data (Breidbach & Maglio, 2020, p. 164). As previously explained predictive analysis is a type of technology that learns from the collected data to predict the future behaviour or decisions of individuals (Siegel, 2013, p. 11).

TikTok states the following, which highlights their analytical practices: “*The more you **engage** with videos on the app, the more **personalized your recommendations** become. From the moment you start your TikTok journey, your first set of likes, comments, and replays will initiate recommendations as the system begins to learn more about your video tastes.*” (TikTok, 2023b).

In view of this, the collected data is analysed by creating profiles of its users, which enable the platform to gain deep knowledge about its users and sell the information to advertisers, which can directly target the relevant potential customers (Huhtala, 2019, p. 56). The ads are then shown by algorithmic recommendation systems, which are based on users' preferences, interests and tastes (Trzaskowski, 2022, p. 449). Therefore, social media platforms use technology, such as algorithms and artificial intelligence, to extract behavioural patterns and use advertising as revenue (Boyer, 2022, p. 1860).

TikTok underlines, that they “[...] provide advertisers with **aggregate information** about the performance of their ads and other content on the Platform in order to help them measure their effectiveness. We create this aggregate information using **Information You Provide, Automatically Collected Information, and Information From Other Sources.** We share your information directly with advertisers where you give us your permission.” (TikTok, 2023g).

Also, Instagram shows personalised ads and measures how the ads have performed (Meta, 2023a). Because of this, Instagram highlights that they “provide advertisers with **reports** about

the kinds of people seeing their ads and how their ads are performing, but we don't share information that personally identifies you.” (Instagram, 2022).

Particularly the fact that information is not shared directly but rather, in an “aggregated form” underlined the point of Sadowski (2019), which described that “regimes of data accumulation” are reinforced through the platform's gatekeeper position (Sadowski, 2019, p. 2). This grants platforms a special and particularly powerful role in the context of the digital risk society.

Against this background, the drive for profit is facilitated through the design and functions of the platform, particularly the algorithmic content curation, which is based on recommendation systems.

As already outlined, the content on the social media platforms is curated by an algorithmic recommendation system based on the personal information extracted (Zeng et al., 2021, p. 3163). The algorithmic recommendation system plays a central role in generating profit. TikTok highlights that the recommendations depend on diverse factors, such as user interactions with content and the personal information collected from its users (TikTok, 2023b). Especially the interaction with content provides so-called “signals”, which assist the recommendation system in understanding the users. The signals are used to create a prediction score, which is an estimation of how likely the user will interact with a video. The videos with the highest score are selected and shown on the For You Page (TikTok, 2023d). The videos are ranked by an algorithm and “weighted based on their value” (TikTok, 2023b). Moreover, content moderation and curation are determined by the terms and conditions set out by the online platforms (Peukert, 2021, p. 22).

Instagram is also based on a recommendation system and functions in a similar way to TikTok. Nick Clegg, the President of Global Affairs at Meta, started a transparency initiative in June 2023 explaining Meta’s AI systems and algorithmic recommendation systems (Clegg, 2023). Similarly to TikTok, Instagram ranks videos based on machine learning models, which use diverse parameters and signals to show personalised content. Instagram highlights that artificial intelligence plays a central role in what people see on the platform (Vorotilov & Shugaepov, 2023). Given this, the ranking process and use of artificial intelligence for the recommendation system is very complex (see Medvedev, Gordon, & Wu, 2019; Vorotilov & Shugaepov, 2023).

Meta describes that for the generation of the Instagram Feed, an artificial intelligence (1) gathers an inventory of available posts (2) leverages “input-signals”, which are data that help to inform the predictions (3) makes predictions based on the signals and (4) ranks posts by a score. The AI then delivers the content to its users based on different predictions, such as how

likely users are to click on the profile of a post's author, how likely the content will be shared and the predicted time spent viewing the content (Meta, 2023d).

Moreover, Meta underlines that the signals and personalised predictions represent the most important components in determining what content is recommended. Signals can be categorised into (1) data specific to the user (e.g. personal data) (2) data specific to the post being ranked (e.g. attributes of the post and creator's) (3) data specific to the user and the post being ranked (e.g. interaction with the post and similar posts) (Meta, 2023e).

As already described in Chapter 4, the profit of data-driven business models is not only generated from the information extracted from the collected data but also from users' **attention**, especially in the context of advertisement (Riesenhuber, 2019, p. 30).

TikTok states the following about algorithmic content curation and the recommendation system: *“This stream of videos is curated to your specific interests, making it convenient to find videos [...]. And **the more you use TikTok, the better the For You feed becomes at curating videos that are tailored to your interests.**”* (TikTok, 2023b).

The economic logic of social media platforms is not only facilitated through the technology used to analyse the data but also through the design of the platform (Schneider, 2018, p. 131).

As seen in **Figures 2 and 3**, the interface of TikTok and Instagram is very similar and centred around videos or images. In this respect, the videos or images nearly fill the entire screen. Zeng et al. (2021) have underlined, that the recommendation mechanisms of TikTok can be described as “one of the most addictive scrolling experiences on the Internet” (Zeng et al., 2021, p. 3163). The platforms are designed in a way which keeps the users as engaged as possible with the personalised content and advertisement (Zeng et al., 2021, p. 1363).

Concluding the analysis has shown that the economic logic behind social media platforms determines the way they function, due to their focus on monetising personal data. Social media platforms can be seen as data-driven business models, which use technology such as artificial intelligence and algorithmic recommendation systems for profit. Given this, the question arises of what it means for society if platforms which provide relevant structures to society are driven by economic logic. In the next part digital risks which are linked to TikTok and Instagram will be outlined. This will be followed by an analysis of how those digital risks are linked to the economic logic of data-driven platform businesses.

6.2 Digital risks and social media

As already elaborated in chapter 3.2.1 (overview of digital risk definitions), the following understanding of digital risks (self-extended definition based on Aven and Renn (2009, p. 6) and Rosa (2003, p. 56)) is applied: *Digital risks refer to the uncertainty about a situation or event and the potential consequences (or outcomes) when something of human value (including humans themselves) is at stake because of digital technologies and the use of technology.*

It must be underlined that the analysis touches upon many digital risks, which have been researched from within diverse disciplines. For that reason, no holistic overview of all studies linked to each specific digital risk can be given. Rather the purpose of this analysis is to highlight studies, which illustrate the digital risks linked to social media. The outlined studies on digital risks will enable an understanding of digital risks posed by social media, how they are facilitated by the economic logic of the platform businesses and what that means for the Digital Service Act, which assigns platform businesses the role of risk regulators.

As outlined in the Digital Service Act systematic risks are linked to VLOPs, such as TikTok and Instagram (see Chapter 4). Due to the large scope of digital risks, the focus will be on the following chosen digital risks outlined in the DSA: (1) misinformation/disinformation (2) mental/physical wellbeing (3) children/ young adults and (4) discrimination and bias.

In that regard, the chosen digital risks have been heavily researched from different perspectives and within diverse contexts (Covid-19, natural disasters, the Ukraine war, US elections, the Ukraine/Russia war etc.). That is why the outlined studies only represent a fraction of the total research and are only illustrated in the context of the research question. Against this background, the link between the economic logic of platform businesses and the digital risks outlined will be touched upon throughout this chapter and summarised in detail in the final chapter of the case study analysis.

6.2.1 Misinformation and Disinformation

The goal of the Digital Service Act for society at large is to mitigate systematic risks, such as manipulation or disinformation (European Commission, 2023b). The European Commission (2022) has defined misinformation as *“false or misleading content shared without harmful intent though the effects can be still harmful.”* (European Commission, 2022). Disinformation on the other hand is defined by the Commission (2022) as *“false or misleading content that is spread with an intention to deceive or secure economic or political gain, and which may cause public harm.”* (European Commission, 2022).

In the following, an illustration of misinformation and disinformation on TikTok and Instagram will be given. The conducted research on recently published studies has revealed that misinformation is mostly studied regarding public health, particularly in the context of the Covid-19 pandemic, whilst disinformation is mainly studied regarding elections and ongoing wars/conflicts. In a first step studies regarding misinformation in the context of the Covid-19 pandemic will be outlined, as the pandemic is a useful example to highlight how digital risks are linked to the economic logic of social media. This will be followed by an illustration of disinformation on social media in the context of the Ukraine/Russia war and the US elections presidential elections in 2016. As already outlined due to the limitations of this thesis the conducted research is only used for illustrative purposes and does not claim to give a holistic overview.

In view of the Covid-19 pandemic, the World Health Organisation has referred to the spread of misinformation as an “infodemic”, which leads to risks for society (see World Health Organization, 2024). Misinformation and disinformation are not a new phenomenon but have been reinforced in the digital age, due to the use of social media as a news outlet, which enables the rapid spread of information to a large audience (Gabarron et al., 2021, 459). Therefore, social media shapes and constructs the public discourse and society's perceptions, attitudes and ideas (Vicari & Komendatova, 2023, p. 2).

Suarez-Lledo et al. (2021) characterised the most dominant topics regarding health misinformation on social media (including TikTok and Instagram). The systematic review revealed that “vaccines, drugs/ smoking, noncommunicable diseases, pandemics, eating disorders, and medical treatments” were the most dominant topics on social media concerning misinformation (Suarez-Lledo & Alvarez-Galvez, 2021, p. 1). Particularly during the Covid-19 pandemic, the effects of social media in the context of misinformation have been demonstrated.

Gabarron et al. (2021) have conducted a systematic review of Covid-19 related to misinformation on social media, which illustrates that social media played a central role in spreading information (accurate information and misinformation) during the “first phase” of the pandemic (Gabarron et al., 2021, p. 455). This aspect is highlighted by the recent study of Baghdadi et al. (2023) on user engagement with misinformation around the Coronavirus on TikTok. In that regard, 166 TikTok videos from the 20th of September 2020 were reviewed, from which 22% contained moderate misinformation and were watched 6.8 million times on average, whilst 7% contained a high level of misinformation, which were viewed around 9.4 million times on average. The study has revealed that videos with moderate misinformation

were less likely to generate user engagement, whilst videos with a high level of misinformation were less likely to be viewed, but if viewed, had a higher user engagement (Baghdadi et al., 2023, p. 1). Also, the study by Southwick et al. (2021) has found that 20-32 % of the analysed Covid-19-related content on TikTok from January to March 2020 contained misinformation. Moreover, 15% of the TikTok videos evoked fear regarding the pandemic (Southwick et al., 2021, p. 234).

The spread of misinformation through social media, particularly in the early stages of the Covid-19 pandemic threatened public health, because it was associated with “increased deaths, wasted resources and delayed treatments” (Quinn, Fazel, & Peters, 2021, p. 573).

The type of content shared on social media is of particular importance. Quinn et al. (2021) carried out a content analysis in early 2020 on Instagram concerning the type of misinformation shared in the context of the pandemic. The content on Instagram contained general mistrust and conspiracy theories, which were linked to questioning authorities by believing that the information regarding Covid-19 were fabricated or hidden by the government or media (Quinn et al., 2021, p. 573).

Whilst social media businesses are not responsible for the content that is shared on their platforms, they are responsible for how the content is distributed. The research paper by Himelein-Wachowiak et al. (2021) has investigated the role of automated accounts or “bots” in spreading misinformation during the Covid-19 pandemic, finding that up to 66% of the analysed bots and unverified accounts on social media (in this case Twitter) were discussing misinformation during the pandemic (Himelein-Wachowiak et al., 2021, p. 1).

Bots are “*fully or semiautomated user accounts operating on social media platforms, which are designed for communication and the imitation of human online-behavior.*” (Bontridder & Pouillet, 2021, p. 5).

In view of this automated systems watch a large amount of the content, which is shared on social media to detect relevant content and recommend it to its users. Academic research on automated systems and algorithmic recommendation systems has shown that divisive content which triggers strong emotions, such as fear, anxiety or hate performs better, which is why algorithms tend to recommend that type of content (Baptista, Rivas-de-Roca, Gradim, & Loureiro, 2023, p. 2; Bontridder & Pouillet, 2021, p. 5; Fernández, Bellogín, & Cantador, 2021, p. 2).

The outlined research underlines, the important role TikTok and Instagram have played in the distribution of misinformation. This role was also highlighted in the context of the US-

presidential elections in 2016 and more recently the spread of misinformation/disinformation in ongoing wars and conflicts, which have illuminated how digital risks are posed by social media to society.

The main research on the US presidential elections in 2016 focuses on the platform “Twitter” (now X) and will be only briefly mentioned as it highlights the role technology played in the distribution of misinformation/disinformation.

The report by Guess et al. (2018) for the European Research Council on the US presidential campaign in 2016 has revealed that *“tendencies toward selective exposure to politically congenial content are likely to extend to misinformation and to be exacerbated by social media platforms”* (Guess, Nyhan, & Reifler, 2018, p. 1).

Bovetand and Makse (2019) carried out a study on the influence of fake news during the 2016 US presidential elections on Twitter and found that 25% of the analysed tweets spread misinformation or extremely biased information, which could have affected the election (Bovet & Makse, 2019, p. 1).

The study conducted by Bessi and Ferrara (2016) found that bots played an important role during the US presidential elections in 2016 with over 400,000 bots engaging in online discussions about the election through approximately 3.8 million tweets, which represent up to one-fifth of the tweets posted from September to October 2016 (Bessi & Ferrara, 2016, p. 11). Moreover, the post-election research has generally described that echo chambers, which will be explained in the later course of this thesis, are filled with “fake news” played a central role in the information distribution during the election (Roberts, Farris, & Benkler, 2018, p. 5).

The report on “the investigation into Russian interference in the 2016 presidential elections” carried out by Mueller (2019) for the U.S. Department of Justice, has claimed that Russia used social media platforms to interfere with the elections (see Mueller, 2019).

Given this, disinformation campaigns on social media have increasingly become a political instrument in times of crisis, intending to manipulate or discredit opponents, such as war enemies (Baptista et al., 2023, p. 2).

The recent war in Ukraine has been titled the “first TikTok war” as mass information on the war was shared on TikTok, shaping the public discourse. In view of this, soldiers used TikTok to report directly on site on the war (Baptista et al., 2023, p. 3). Moreover, TikTok was used to cover the conflict by individuals on-site or by influencers, spreading information (Sidorenko, Alonso López, & Paíno Ambrosio, 2023, pp. 744–745).

The study conducted by Primig et al. (2023) found that war-related content on TikTok leads to the mediation of distant suffering through using TikTok's editing functions, such as sound or filters, to provoke an emotional response in the audience (Primig, Szabó, & Lacasa, 2023, p. 1). Weimann (2021) has shown that the TikTok recommendation system pushed its users who unintentionally watch disturbing content, to watch more of that content as it keeps the user more engaged, due to strong emotions (Weimann & Masri, 2021, p. 697).

In the context of the Digital Service Act, the European Commission has published a report on "the application of the risk management framework to Russian disinformation campaigns" (European Commission, Directorate-General for Communications Networks, Content and Technology, 2023). The report claims that social media businesses enabled Russia *"to run a large-scale disinformation campaign targeting the European Union [...]"* (European Commission, Directorate-General for Communications Networks, Content and Technology, 2023, p. 7). The analysis revealed that disinformation reached an aggregated audience of 165 million social media users and generated 16 billion views in 2022 (European Commission, Directorate-General for Communications Networks, Content and Technology, 2023, p. 7). The largest audiences were reached through Meta's platforms (e.g. Facebook and Instagram), whilst the numbers of "pro-Kremlin channels" on TikTok doubled since the start of the war (European Commission, Directorate-General for Communications Networks, Content and Technology, 2023, p. 11). The study highlights that from January until May 2023, the posting activity of "pro-Kremlin accounts" increased to 34 % on TikTok (European Commission, Directorate-General for Communications Networks, Content and Technology, 2023, p. 12).

The report concludes that the efforts of social media platforms (including TikTok and Instagram) were unsuccessful in preventing the spread of disinformation. The report underlines that this is not only concerning regarding the war but also opens up questions about the integrity of the European elections in 2024 (European Commission, Directorate-General for Communications Networks, Content and Technology, 2023, p. 7).

As outlined the spread of misinformation is influenced by diverse factors, such as user's engagement with the content, content creators/influencers who generate misinformation, user's adaptive behaviour, emotions of users, bots and malicious accounts, and the algorithmic recommendation system (Pathak, Spezzano, & Pera, 2023, p. 2). In view of this, algorithms and technologies, such as artificial intelligence enable individuals to create misinformation /disinformation. Additionally, contributing to spreading the information (Bontridder & Pouillet, 2021, p. 1).

Ceylan et al. (2023) have illustrated in their recent research that “the structure of online sharing built into social platforms is more important than individual deficits in critical reasoning and partisan bias” (Ceylan, Anderson, & Wood, 2023, p. 1). Due to the reward-based learning system on social media, users form habits of sharing information, which attract other users’ engagement. Since sensational content usually performs better, the reward-based system can be seen as one of the main driving forces for the spread of misinformation (Ceylan et al., 2023, p. 1).

Sun (2023) has underlined that disinformation is increasingly “created and disseminated by social media algorithms” (Sun, 2023, p. 367). Algorithmic recommendation systems are not designed to inform their users, but rather to keep them engaged and satisfied, generating profit out of the advertisement shown in the news feed (Fernández et al., 2021, p. 8; Pathak et al., 2023, p. 2).

In view of these two types of algorithms must be differentiated (1) recommendation algorithms and (2) generative algorithms. Recommendation algorithms can be categorised based on the way they filter information (Sun, 2023, pp. 374–380). Algorithms can either employ collaborative filtering, content-based filtering, or a hybrid filtering system. Collaborative filtering is based on identifying the preference of a large group and recommending content to users, which are characterised as part of the group based on the group’s preference. Content-based filtering focuses on recommending content similar to content which users have already shown interest in. The hybrid system combines both filtering systems (Sun, 2023, p. 374).

Benzie and Montasari (2022) have highlighted how the use of AI (through software robots) in social media is linked to the distribution of misinformation/ disinformation. They outlined how AI and the programmed algorithms recommend misinformation content to users who are likely to engage with that type of content, as the AI is programmed to show its users information which they would engage with (see Benzie & Montasari, 2022).

Thus, recommendation algorithms can spread and amplify disinformation/misinformation, whilst generative algorithms can enable individuals to generate disinformation, mostly in the form of so-called deepfakes (Sun, 2023, p. 377).

Deepfakes can be defined as “digitally manipulated synthetic media content (e.g., videos, images, sound clips) in which people are shown to do or say something that never existed or happened in the real world.” (Mustak, Salminen, Mäntymäki, Rahman, & Dwivedi, 2023, p. 1). They are generated by algorithms and are distributed on social media platforms (Mustak et al., 2023, p. 11).

The research on deepfakes is still very limited, as they have only recently become popular since the technologies to create deepfakes have become more accessible to the public. In that regard, deepfakes were mainly used for fake porn and celebrities, which has changed since deepfakes were also used in the Ukraine war. This highlights that deepfakes have political implications and can become a threat to democracy in the future, especially when the technologies are becoming better, making it impossible for users to differentiate between fake and real content (Pawelec, 2022, pp. 1–2; Twomey et al., 2023).

In view of this, TikTok and Instagram have recognised the risks of misinformation and disinformation on their platforms and have taken actions to protect their users (see Meta, 2019; TikTok, 2023k).

In that context, TikTok states the following: *“We recognize the impact misinformation can have in eroding trust in public health, electoral processes, facts, and science. We are committed to being part of the solution. We treat misinformation with the utmost seriousness and take a multi-pronged approach to stopping it from spreading, including working with independent fact-checking organizations.”* (TikTok, 2024a).

TikTok uses automated content moderation and human reviewers to detect misinformation/disinformation and prevent it from spreading. The content is either completely removed from the platform or flagged by TikTok as containing misinformation (similar to Instagram see **Figure 4**) (TikTok, 2024a).

The content moderation on TikTok is mainly based on automated systems. Content which is uploaded on TikTok is **first reviewed by the automated moderation technology**, which aims to identify content that violates the Community Guidelines. If a violation is identified either it is automatically removed, or in cases where the degree of confidence in violation is smaller, the content gets passed on to the safety team (human review) (TikTok, 2024b).

TikTok partners, since 2020, with 15 fact-checking organisations, which are verified signatories of the International Fact-Checking Networks. The fact-checking organisations, do not moderate content and only provide input with their assessments helping TikTok *“to take appropriate action that upholds [...] Community Guidelines”* (TikTok, 2024a).

TikTok describes the key principles on which automated and human content moderation is based, in its DSA transparency report. The following four pillars guide content moderation:

“1. Remove violative content from the platform that breaks our rules (noting that we do not allow several types of mature content themes, including gory, gruesome, disturbing, or extremely violent content);

2. Age-restrict mature content (that does not violate our Community Guidelines but which contains mature themes) so it is only viewed by adults (18 years and older);

3. Maintain For You Feed eligibility standards to help ensure any content that may be promoted by the recommendation system is appropriate for a broad audience; and

4. Empower our community with information, tools, and resources.” (TikTok, 2023j, p. 3).

Instagram describes similar efforts to combat misinformation on its platform. The platform also works with third-party fact-checkers and automated technology to remove or label content rated as false information, as shown in **Figure 4** (Meta, 2019). The DSA transparency report of Instagram specifies that **in most cases content and accounts are removed automatically**. Because of this, the technology selects the content for human review and ranks the content by prioritising the most critical content to be reviewed (Instagram, 2023b, pp. 8–9).

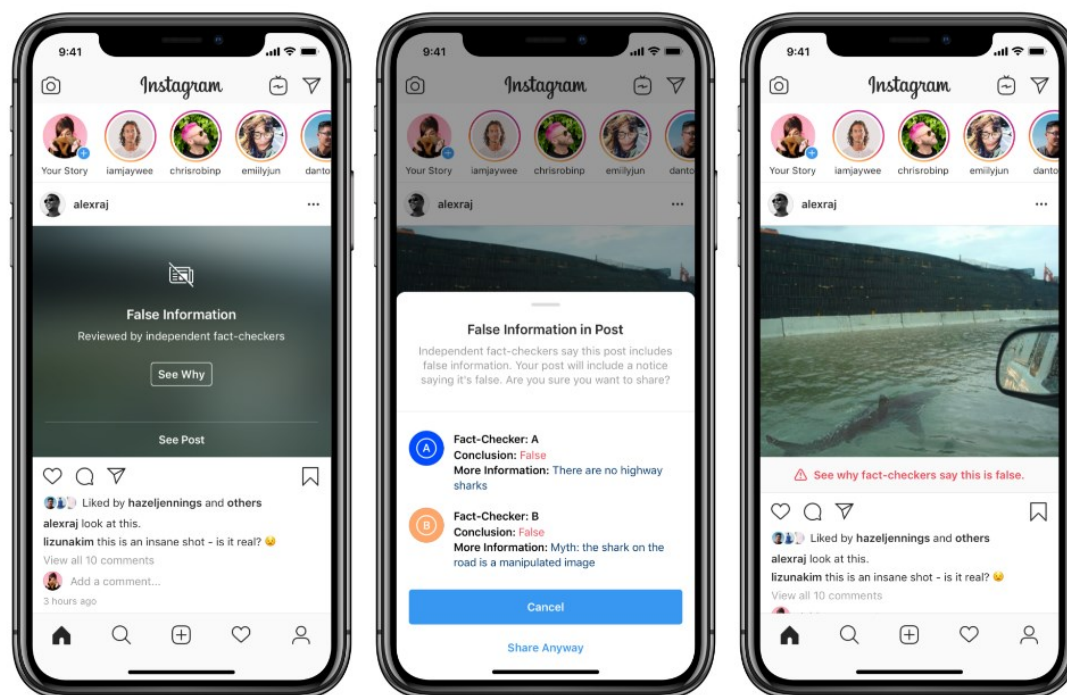


Figure 4 Misinformation on Instagram (Meta, 2019)

Instagram reveals in their DSA transparency report that between April and September 2023, 76.298.413 million pieces of content were removed, from which 75.113.462 million pieces were removed automatically (Instagram, 2023b, p. 10).

TikTok on the other hand describes that for September 2023 the total number of content removed was 3.999.960 million, whilst 1.800.826 million pieces of content were removed by the automated technology on TikTok (TikTok, 2023j, p. 9).

The outlined numbers published by Instagram and TikTok are particularly interesting when being compared. On Instagram, most of the content is removed by the automated systems, whilst TikTok claims that only 1.800.826 million videos were removed automatically leaving, 2.199.134 from the total number being reviewed by humans in September 2023 (Instagram, 2023b; TikTok, 2023j, p. 5). This is particularly striking, as it is unclear why the aspect of automated removal differs between the two platforms, even though they use nearly the same technology and function similarly. Moreover, TikTok states on its website, that the platform mostly relies on automated systems regarding content moderation, as all content is first reviewed by automated technology (TikTok, 2024b). Without going into detail as this would be speculative, it is worth mentioning this aspect as it is unclear to what extent the information provided by the platforms to the public is accurate. This aspect is striking and underlines, that the research relies on the information given by the businesses, as the information published cannot be verified and leaves it unclear why the two platforms provide information which are opposing.

In view of that TikTok claims that the automated content moderation has an accuracy rate of 94 % and an error rate of 6% in September 2023 (TikTok, 2023j, p. 4). Instagram also recognises the error rates in the DSA transparency report but does not give any concrete information on the error or accuracy rate (Instagram, 2023b, pp. 15–16).

Content is not only removed by the platforms but can also be restricted. In that regard, 13.975.378 million pieces of content were restricted by TikTok in September 2023 based on TikTok's community guidelines (TikTok, 2023j, p. 8). Given this 2.136 videos were removed due to misleading or false content, from which 698 videos were removed by automated systems (TikTok, 2023j, p. 9). Instagram does not provide any information on how much content was restricted by the platform generally or in the context of misinformation or disinformation (Instagram, 2023b).

The platforms do not only remove and flag content but also provide its users with sources, which will be outlined for Instagram in the part on physical and mental wellbeing. TikTok states the following, recognising the effect the platform has on society, by naming sources related to the digital risks outlined in this part:

“As well as taking steps to protect our community from harmful misinformation, we've connected people to authoritative sources of information on issues such as Covid-19, the Holocaust, and the war in Ukraine.” (TikTok, 2023k).

In summary, the outlined studies on the role of social media in the context of misinformation/disinformation have underlined, that risks arise out of the way information is distributed to the users by the platforms, which shape public discourses and can have negative effects on democracy. In that regard, it is important to highlight, that social media algorithms do not cause misinformation/disinformation, but play a central role in enabling its users to generate misinformation/disinformation and distribute that information to a targeted large audience in a very short time (Grandinetti & Bruinsma, 2023, p. 288). Moreover, this part has highlighted the role automated systems play in regulating the risks of misinformation/disinformation, as the platforms rely mainly on automated technologies for their content moderation.

6.2.2 Physical and Mental Wellbeing

Social media has been linked to negative effects on physical and mental wellbeing. The current research highlights that social media plays an important factor in contributing to mental health issues. Nevertheless, the research on how and why social media has an impact on mental health is still very limited and fragmented (Dutt, 2023, p. 355; Moreton & Greenfield, 2022, p. 1). The effects of social media on physical and mental wellbeing have particularly been studied by disciplines such as psychology, behavioural science, and medical science. In the following an overview of some relevant studies published in academic journals from the disciplines mentioned will be outlined, noting that the methods used in the studies cannot be explained or fully grasped, due to a lack of expertise. Montag, Yang and Elhai (2021) have highlighted, that the psychological research on TikTok users is limited, which makes it too early to speculate on the correlation of psychological effects (Montag, Yang, & Elhai, 2021, p. 3). That is why the focus in this part will be on Instagram, as the research and evidence in psychology are mostly based on long-term studies, which are still very limited regarding TikTok.

Faelens et al. (2021) have given a systematic overview of research “on the relationship between Instagram use and indicators of mental health issues” (Faelens et al., 2021, p. 1). The review has revealed that the use of Instagram could be linked to mental health issues such as depression, anxiety, addiction and eating disorders (Faelens et al., 2021, p. 4). The most evidence was found for the relationship between Instagram use and poor body image/eating disorders (Faelens et al., 2021, p. 1).

Also, Keles et al. (2020) have given a systematic overview of research on the influence of social media on depression, anxiety and psychological distress of young adults. They classified four factors which have negative effects on mental health (1) time spent on social media (2) active or passive social media behaviour (3) (mental) investment and (4) social media addiction (Keles et al., 2020, p. 79).

Their review has underlined the positive correlation between increased social media use and depression, anxiety, and psychological distress. The more time users spend on social media, the more likely they are to experience negative psychological symptoms (Keles et al., 2020, pp. 87–88). A study conducted by Keyte et al. (2021) on the intensity of Instagram use and wellbeing supports the findings since, the research has shown, that individuals who spend more time on Instagram, report poorer mental wellbeing (Keyte et al., 2021, p. 436).

Furthermore, the study conducted by Sherlock and Wagstaff (2019) on the relationship between the psychological wellbeing of women and the frequency of Instagram use has highlighted that a correlation between depressive symptoms, anxiety and body dissatisfaction could be found (Sherlock & Wagstaff, 2019, p. 482).

Research regarding the activity of users remains mixed as some results suggest a correlation between depressive moods in both active and passive use, whilst others suggest a higher correlation between depression and the passive use of Instagram (Keles et al., 2020, pp. 87–88; Keyte et al., 2021, p. 437). Finally, a high level of mental investment in social media content and addiction to social media have been shown to correlate with anxiety and depressive moods for young adults (Keles et al., 2020, pp. 87–88).

Chatzopoulou et al. (2020) focused their research on young male Instagram users, in the context of body images and fitness (“the Instabod”), as the research has been limited regarding male users in comparison to female users in the context of body image. The study has revealed that Instagram can have positive effects, such as a higher motivation to stay fit, but can also have negative effects on mental health through competition, which leads to anxiety and body dysmorphia symptoms (Chatzopoulou et al., 2020, p. 1270). The content viewed, about fitness, was mostly based on one ideal body type and filled with advertisements when searching for fitness and health information (Chatzopoulou et al., 2020, pp. 1273–1274).

Instagram’s focus on image-based content (e.g. photos and videos), has been linked to negative effects on body images and eating disorders. The viewed content, particularly “comparison material” or fitness inspiration content viewed on Instagram is linked to negative effects on mental health (Faelens et al., 2021, p. 12). Moreover, Instagram gives “ordinary” people a

platform to present their lives in an idealised version by using filters and other forms of editing, which promotes social comparison and has negative effects on user's mental health (Sherlock & Wagstaff, 2019, p. 483).

In that regard photo manipulation, such as editing and beauty filters on Instagram can harm the body image of users and appearance in general, promoting unrealistic ideals. That is particularly the case for young adults who engage in photo editing (Mancin, Cerea, Bottesi, & Ghisi, 2023, pp. 1–3; McGovern, Collins, & Dunne, 2022, p. 505).

The outlined research has underlined that the effect of Instagram on mental and physical health depends on diverse factors, such as the intensity of use, type of use and content watched. In view of this, the relationship between social media use and mental/ physical health is very complex. That is why it would be simplified to state that social media is the cause of negative effects on mental and physical health. Rather the conducted research has revealed that Instagram is a contributing factor, which can reinforce negative effects on physical and mental health (Faelens et al., 2021, p. 1).

Furthermore, the qualitative study conducted by Moreton and Greenfield (2022) on university student's views on the impact of Instagram on mental wellbeing has revealed that Instagram has implications on mental wellbeing because of ideals that are perpetuated (e.g. body images or lifestyle), cyberbullying and social acceptance (Moreton & Greenfield, 2022, p. 7).

Lambert, Barnstable, Minter, Cooper and McEwan (2022) have studied the effects of a one-week break from social media (including Instagram and TikTok) on wellbeing and shown that the break from social media has led to a significant improvement in wellbeing, anxiety and depression of the participants. It must be noted, that the study was conducted based on 154 participants for only one week, which can give indications but is not necessarily representative of a large population over a longer period (Lambert, Barnstable, Minter, Cooper, & McEwan, 2022, pp. 287–288).

Nevertheless, the outlined studies highlight the negative effects of social media on physical and mental beings, which raises the question of why social media, like Instagram and TikTok, could potentially have those negative effects outlined. McCashin and Murphy (2023) have highlighted that the built-in mechanisms of TikTok are based on using emotions and user motivation, such as self-expression or self-optimisation to produce content which keeps the users as engaged as possible (McCashin & Murphy, 2023, p. 281). This aspect can be linked back to the economic logic of the platform, as it generates profit out of its user's attention and engagement with the content (Riesenhuber, 2019, p. 30). Social rewards and emotions are used to gain its user's

attention creating an addictive structure, which poses risks to its users (Dutt, 2023, pp. 361–362).

A recent study conducted by Dondzilo et al. (2023) on the TikTok recommendation system regarding eating disorders has highlighted that individuals with eating disorder symptoms or individuals who engage with eating disorder content or appearance content are more likely to get a higher proportion of content, which shows appearance or eating-related content, recommended by the TikTok algorithm (Dondzilo et al., 2023, pp. 2–4).

Moreover, particularly the use of social media for mental health advice has been linked to diverse risks, due to misinformation, self-diagnosis, and misleading health information. In that regard, social media platforms promote popular content, such as mental health advice regardless of its quality (Naslund, Bondre, Torous, & Aschbrenner, 2020, p. 251).

TikTok acknowledges the negative effects of their technology by providing resources to users searching for suicide content and publishing advice on addiction, overuse of the app, eating disorders and digital well-being (TikTok, 2024c).

Moreover, TikTok and Instagram remove and restrict content in the context of negative effects on physical and mental wellbeing. In September 2023, TikTok removed 510.836 videos which violated the community guidelines concerning mental and behavioural health, from which 253.411 were removed automatically (TikTok, 2023j, p. 9). Instagram removed 153.051 thousand pieces of content related to suicide and self-injury from April to September 2023, from which 121.530 were removed automatically (Instagram, 2023b, p. 10).

In this context, it must be noted that TikTok and Instagram do not only have negative effects on individuals but can also be beneficial for its users. Studies have shown that users with moderate or severe depression prefer to use social media to facilitate social interactions, find a community or seek help in the form of online consultation (Naslund et al., 2020, p. 246). Moreover, TikTok and Instagram do not only contain content which facilitates negative effects on mental and physical health. For example, Ebrahim and Tanner (2023) have pointed out how female unrealistic standards of beauty are challenged through educational content on TikTok (Ebrahim & Tanner, 2023).

To conclude the outlined studies have highlighted, that TikTok and Instagram are likely to impact their user's physical or mental wellbeing, based on how the platforms are structured and functioning, particularly based on their algorithmic recommendation systems and personalised feeds.

6.2.3 Children and Young Adults

The Digital Service Act has specifically focused on minors, as VLOPs (e.g. social media) can pose particular risks to children and young adults (European Union, 2022, p. 64).

In view of this TikTok is an important example as the platform specifically targets teens and pre-teens (Zeng et al., 2021, p. 3162). TikTok and Instagram state in their official policy that the minimum age of use is 13 and above (Instagram, 2021; TikTok, 2023h). Nevertheless, TikTok is the most used social media platform among children and young adults (McCashin & Murphy, 2023, p. 279). TikTok is mostly used “among the age groups of 12 to 17, with more than one-quarter of daily users being under the age of 14” (Bahnweg & Omar, 2023, p. 1). Instagram on the other is used among an audience in the age range of 18-34, whilst the most active users are between 18-24 years old (Statista, 2024). This part will mainly focus on TikTok, as it is a more powerful example of highlighting the risks for children and young adults.

Social media platforms like TikTok have become a space for socialisation, which influenced the development of children and young adults (Soriano-Ayala, Bonillo Díaz, & Cala, 2023, p. 211). TikTok is used by young adults to satisfy their needs through entertainment, connecting with friends, expression of their personality and being up to date with relevant pop culture (e.g. challenges, trends etc.). Moreover, the reason for the use of TikTok is linked to a “fear of missing out”, as the topics discussed on the platform become relevant for young adults to be able to participate in pop-culture and subculture (Pedrouzo & Krynski, 2023, p. 4).

Social media is linked to opportunities, such as education or identity exploration, but also to challenges for young adults such as online bullying, effects on body images or misinformation (Taylor & Brisini, 2024, p. 1). The negative effects on young adults are particularly dangerous due to a high vulnerability during puberty or childhood (Sagrera et al., 2022, p. 2).

In general, the excessive use of the internet has been linked with physical inactivity and obesity, sleep disturbance and a minimised attention span. TikTok’s algorithm is designed in a way to make content consumption as addictive as possible by enabling it to consume as much information as possible in a very short time, through scrolling down content which is 15 seconds to 1 minute long. Moreover, the personalisation of the For You Page makes TikTok attractive for active and passive social media users (Pedrouzo & Krynski, 2023, p.2-3).

As already outlined in the part on mental and physical wellbeing social media can have negative effects on its users. In view of this, the type of content shown to users is of particular

importance. That is why TikTok has been linked to effects on self-harm, suicide, body image issues and eating disorders (Bahnweg & Omar, 2023).

Particularly challenges on TikTok, which users are supposed to attempt, have been linked to dangers for children. The so-called “blackout challenge” for example animated young users to hold their breath until they passed out, which has led to several deaths in the United States (Fung & Wong, 2023, p. 1; Pedrouzo & Krynski, 2023, p. 3). Another example is the more recent “Labello challenge”, which had many views in France and Belgium. The challenge animated young adults to remove a piece of the lipstick when they were feeling depressed. When the Labello was finished the participants were animated to practice self-arm (Bahnweg & Omar, 2023, p. 2).

Not only the dangerous challenges are posing risks to children and young adults, but also the accessibility to content promoting questionable values or behaviour to minors poses risks.

A study conducted by Russel et al. (2021) on how alcohol is portrayed on TikTok has revealed that the top videos on TikTok promote a rapid consumption of multiple drinks as alcohol consumption is associated positively. The negative effects of alcohol use are rarely discussed in the content shown by TikTok (Russell et al., 2021, p. 615). The content was accessible without an age verification, which suggests that there are no measures to limit underage youth exposure to content promoting the use of alcohol (Russell et al., 2021, p. 619).

Moreover, a study conducted by Ayalde et al. (2023) on how energy drinks have been portrayed on TikTok has shown that from 197 videos analysed (70 + million views), 29% were linked to advertisement and sponsorship, whilst 22% featured a child or young adult. Generally, the study showed, that energy drinks are mainly portrayed positively, promoting energy drinks to minors (Ayalde et al., 2023, p. 633).

Furthermore, a study conducted by Soriano-Ayala et al. (2023) on the hypersexualisation of children on TikTok has revealed that sexualisation is seen as intrinsic to the platform by its users. This is linked to the platform being centred around the body, especially in the context of dance videos. TikTok increases the manifestation of sexual behaviour in minors, as the platform emphasises sexual value, particularly for young women, by recommending sexualised content as it generates more user engagement (Soriano-Ayala et al., 2023, pp. 210–214). Spaccatini (2019) has highlighted based on a systematic review how early sexualisation can have negative effects on young adults, especially in the context of body image and identity (see Spaccatini, 2019).

The recommended content is based on personalised predictions of how likely a user will engage with the content, which is why inappropriate content could be recommended to children and young adults. The TikTok algorithm grabs its user's attention and generates stimulation and dopamine, which makes the platform highlight addictive. TikTok is characterised based on the focus on its algorithmic recommendation system, which is one of the most powerful prediction systems, driving the personalised user experience (Pedrouzo & Krynski, 2023, p. 4).

TikTok recognises the risks personalised recommendation systems pose to children and states, only a limited amount of personal data is collected from children. In view of this, TikTok recognises that children are registered on the platform (TikTok, 2023a).

TikTok states: *“We use the information we collect to provide and support our services. For example, we use username and password to authenticate Children. We may use the information that is collected automatically to provide personalized content; serve contextual advertising; perform analytics and troubleshoot; protect the security and integrity of the user and our services; and ensure legal and regulatory compliance.”* (TikTok, 2023a).

The Data Protection Commission (DPC) fined TikTok in September 2023 with 345 million euros, due to failing to protect children. TikTok has set children's accounts by default to public settings and failed to recognise the risks for children on their platform. In addition, the DPC has found that TikTok implemented so-called dark patterns, which nudge users towards choosing a more intrusive privacy setting when registering for the platform, which poses specific risks to children (Data Protection Commission, 2023).



Figure 5 Content restriction on Instagram (Instagram, 2024a)

Against this background, it must be noted, that TikTok and Instagram have implemented strategies for protecting children and young adults. TikTok has removed 807.051 pieces of content regarding youth safety and wellbeing in September 2023. No numbers were given on how much of that content was removed automatically because youth safety is considered alongside all subcategories outlined in the DSA transparency report (TikTok, 2023j, p. 9). Instagram on the other hand, has removed 107.518 thousand pieces of content in the context of child endangerment, from which 30.963 thousand pieces of content were removed automatically (Instagram, 2023b, p. 10).

Moreover, TikTok and Instagram have implemented strategies to protect minors. For example, not providing certain features to

users younger users (aged 13-17) (Instagram, 2021; TikTok, 2023f). In addition, content related to challenges which have been linked to dangers is removed from the platform, such as the outlined blackout challenge. When searching for the challenges TikTok provides the user instead with information and resources regarding mental and physical health (see **Figure 5**). Also, Instagram has acknowledged potential negative effects and published information regarding safe use by providing information on eating disorders and self-harm, time spent on Instagram and cyberbullying (Instagram, 2024).

In summary, TikTok and Instagram pose specific risks to children and young adults, who represent most users on the platforms. Through recommendation systems and algorithmic content curation, the platforms tend to be highly addictive and influential on the development of young adults.

6.2.4 Discrimination and Bias

Lastly, this part will outline studies regarding discrimination and bias on Instagram and TikTok. Discrimination on social media can be actualised through the distribution of discriminatory content or the technological systems used by the platforms. The focus of this thesis will be on discrimination and bias through technological systems, which is why discriminatory content is only mentioned briefly. In view of this, it must be highlighted, that the general literature on algorithmic bias and discrimination has a wide range, nevertheless the research regarding discrimination and bias on TikTok and Instagram is still limited. Due to the large amount of research conducted regarding algorithmic discrimination and bias, this part only highlights some aspects, which will be extended in the following chapter.

Discriminatory content and hate speech on social media are increasingly having an impact on society and democracy. This was particularly visible in the context of the Covid-19 pandemic, which is highlighted in the study by Jacques et al. (2023) on racial discrimination against Asians and Asian Americans during the pandemic on TikTok (Jacques et al., 2023). The study revealed that discriminatory content and hate speech of Asians and Asian Americans was distributed on TikTok amplifying racial discrimination and abuse stories (Jacques et al., 2023, p. 4).

The Council of Europe (2024) has defined hate speech as the following: *“Hate speech covers many forms of expressions which advocate, incite, promote or justify hatred, violence and discrimination against a person or group of persons for a variety of reasons.”* (Council of Europe, 2024).

A study conducted for the European Parliament (2021) on “The Impact of Disinformation Campaigns About Migrants and Minority Groups in the EU” has revealed that ethnic, religious and cultural minorities have been specifically targeted through disinformation campaigns on social media platforms (Szakács & Bognár, 2021, p. vi).

Burton (2023) shows how artificial intelligence can contribute to the polarisation and radicalisation of social media users (Burton, 2023, p. 1). Particularly activities of Al Qaeda and ISIS have gained public attention in radicalising young social media users. Also, far-right organisations have been radicalising users through social media, as their extreme content is recommended by the algorithmic systems, due to grabbing its user's attention by triggering strong emotions (Burton, 2023, p. 3). Social media not only enables the distribution of discriminatory content but also influences democracy through shaping users' beliefs and ideas. This aspect is linked to the algorithmic recommendation systems, filter bubbles and echo chambers (see Pariser, 2012). Echo chambers describe that social media users mainly engage “like-minded others and ideologically-aligned content, thus rarely being exposed to conflicting ideas” (Terren & Borge, 2021, p. 100). Filter bubbles on the other hand describe a form of echo chamber, which is produced by algorithms through personalisation, without any active choice of the user on how content and information are distributed to them (Ross Arguedas et al., 2022, p. 11).

The conducted literature review by Ross Arguedas et al. (2022) on filter bubbles and echo chambers has revealed that little empirical research has been done regarding echo chambers and filter bubbles. Nevertheless, the review has revealed that it is likely that filter bubbles and echo chambers could affect polarising social media users (Ross Arguedas et al., 2022, pp. 29–30).

TikTok and Instagram are not only enabling the distribution of discriminatory content but have also been accused of discriminatory practices, through biased algorithmic recommendation systems (Bouchardet, 2023, pp. 1–2; Peterson-Salahuddin, 2022, p. 5).

The study conducted by Botero Arcila and Griffin (2023) for the European Parliament on “Social Media Platforms and Challenges for Democracy, Rule of Law and Fundamental Rights” has highlighted discriminatory practices of social media platforms (Botero Arcila & Griffin, 2023). The study outlines how automated and manual content moderation is linked to biases against marginalised groups. The study underlines that for example, face recognition software is less accurate for women and that language analysis software is less accurate for minority

groups with dialects or slang, as the training data used by social media platforms does not represent marginalised groups (Botero Arcila & Griffin, 2023, p. 54).

A study conducted by Sap et al. (2019) on the risk of racial bias on Twitter (now X) has found that the social media algorithm was more likely to flag or remove content if the content contained African American English dialect (Sap et al., 2019). This was also the case for the TikTok algorithm (Harris, Johnson, Palmer, Yang, & Bruckman, 2023, p. 3).

Also, Instagram's content moderation has been increasingly criticised for discriminatory practices based on the algorithmic systems which discriminate against marginalised groups, such as racial or gender minorities (Bouchardet, 2023, p. 1).

Are (2020) has highlighted that Instagram censors women through algorithmic censorship in the context of women's bodies, nudity and sexuality. The study has shown, that content of women Carnival dancers or women athletes has been censored by Instagram, due to flagging it as "inappropriate content", even though it did not violate the community guidelines (Are, 2020, pp. 741–742).

Moreover, Bouchardet (2023) has outlined that Instagram's content moderation entails a form of "automated coloniality", which describes how technology amplifies and perpetuates mechanisms of coloniality (Bouchardet, 2023, p. 4). The study found that the content moderation of Instagram "systematically presents discriminatory effects" (Bouchardet, 2023, p. 13).

Similar studies can be found regarding TikTok. The study by Sannon et al. (2023) has highlighted that content from disabled users faces algorithmic suppression on TikTok by flagging content inaccurately as violating the terms of services (Sannon et al., 2023, p. 7).

Peterson-Salahuddin (2022) has highlighted that marginalised content creators, such as "black, brown, fat, queer, and disabled creators" have been affected by algorithmic discrimination on TikTok (Peterson-Salahuddin, 2022, p. 1). Also, the study conducted by Haimson et al. (2021) has revealed that the content and accounts of transgender people and black people were more likely to be removed compared to other groups on social media sites (including Instagram and TikTok) (Haimson et al., 2021, p. 1).

Because of this particularly black content creators have addressed algorithmic bias and discrimination on TikTok. The content creator "Ziggi Tyler" has shown in a video how the terms "Black Lives Matter" were flagged by the platform, whilst "white supremacy" was not flagged by the automated systems. TikTok has reacted to the accusations by stating that this was a

“glitch” in the system and is not representative of their algorithmic recommendation system (Peterson-Salahuddin, 2022, p. 6; Wahid, 2023, p. 108).

Also, the qualitative study conducted by Harris et al. (2023) on the experience of black content creators on TikTok has revealed, that the content moderation on TikTok challenges black content creators, as their content is more likely to be suppressed or removed by TikTok. In that regard, TikTok has placed content “under review”, which many of the participants of the study experienced (Harris et al., 2023, pp. 11–13). Moreover, the study has revealed that:

“[...] creators identified a phenomenon of videos and live-streams on TikTok not being placed under any formal review or violation, but also not being shown to anyone, even for creators with hundreds of thousands of followers. [...] This phenomenon seems especially common when creators discuss topics related to Black identity or other marginalized identities.” (Harris et al., 2023, p. 13).

Wahid (2023) has outlined that social media facilitated discriminatory practices based on creating social categories, which inform the algorithms and generate biased technological systems (Wahid, 2023, p. 109). Bechman and Bowker (2019) have outlined how programmed classifications in deep learning mechanisms for artificial intelligence and automated practices on social media can reinforce discrimination (Bechmann & Bowker, 2019, p. 8).

Given this, algorithmic bias on social media platforms reinforced discrimination, which Agan et al. (2023) have investigated. Their study shows how algorithms trained with human behavioural data can misunderstand the prejudice of social media users, generating biased algorithms (Agan et al., 2023, p. 2).

In view of this, the research on algorithmic recommendation systems is particularly challenging as they lack transparency (e.g. “black box”), which is why the empirical evidence is still very limited. Peterson-Salahuddin (2022) underlines, that “the actual existence of racial bias in algorithms can never be truly known”, due to the “proprietaries nature of the algorithms” (Peterson-Salahuddin, 2022, p. 6).

To conclude, the outlined studies have illustrated that the algorithmic recommendation systems of TikTok and Instagram are linked to discriminatory practices, which are mainly based on algorithmic bias. Against this background, it is important to highlight, that no information on Meta’s/ Instagram’s or TikTok’s website regarding algorithmic bias or discrimination could be found.

The analysis of the outlined digital risks (misinformation/disinformation, negative effects on mental/physical wellbeing, negative effects on children and young adults, discrimination/ bias) has already touched upon how the risks are interwoven with the technological systems used by the platforms. In the following, this aspect will be extended by connecting the outlined digital risks with the economic logic of the platform businesses. The adoption of this approach will facilitate our capacity to address the research inquiry presented.

6.3 Digital risks and the platform economy

In the previous part of this thesis digital risks posed by social media platforms to society were discussed. The focus was set on understanding how the digital risks are interwoven with the technological systems used by the platforms. In the following, this will be linked back to the economic logic of data-driven platform businesses, which was already touched upon during the digital risk analysis. Nevertheless, this aspect will be outlined in more detail, showing that the technologies used and thus the digital risks represent an essential component of the economic logic of the platform businesses. Given this the research question “*How are digital risks, which arise from social media platforms linked to the data-driven value creation within the platform economy?*” will be answered, followed by a discussion of the implications in the context of the DSA and the digital risk society.

As already outlined in the previous chapters social media platforms can be characterised as data-driven platform businesses, which collect, extract and analyse personal data as the key resource of their business model (Srnicsek, 2017, pp. 254–255). In view of this social media platforms like TikTok and Instagram monetise personal data, by using technologies, which are linked to digital risks. In this context platform businesses usually use so-called “end-user licensing agreements”, which describe the agreement of the users to the terms and conditions of the platforms. Given this, users must accept the terms and conditions to be able to use the services provided by the platforms. Those agreements are characterised as being one-sided and thus not open for negotiations (Sadowski, 2019, p. 7). This agreement grants the platform legal access to the data of its users (Rodríguez de las Heras Ballell, 2021, p. 82).

In May 2023 Meta was fined 1.2 billion euros by the Irish Data Protection Authority for violating data protection rules in the European Union, by sharing and transferring personal data of European users (European Data Protection Board, 2023a). Moreover, Meta was already fined 180 million euros in January 2023 in the case of Instagram by the Irish Data Protection Authority for their unlawful processing of personal data for behavioural advertising, which highlighted the important impact Instagram has on its users based on the processing of personal

data (European Data Protection Board, 2023c). The European Data Protection Board (EDPB) adopted a binding decision in Oktober 2023, as Meta was found to not have complied with orders imposed by the EU. The decision *“imposes a ban on processing personal data for behavioural advertising on the legal base of contract [...]”* (European Data Protection Board, 2023b). In this context, Meta has proposed “a consent-based approach” (see **Figure 6**) as the legal basis (European Data Protection Board, 2023b).

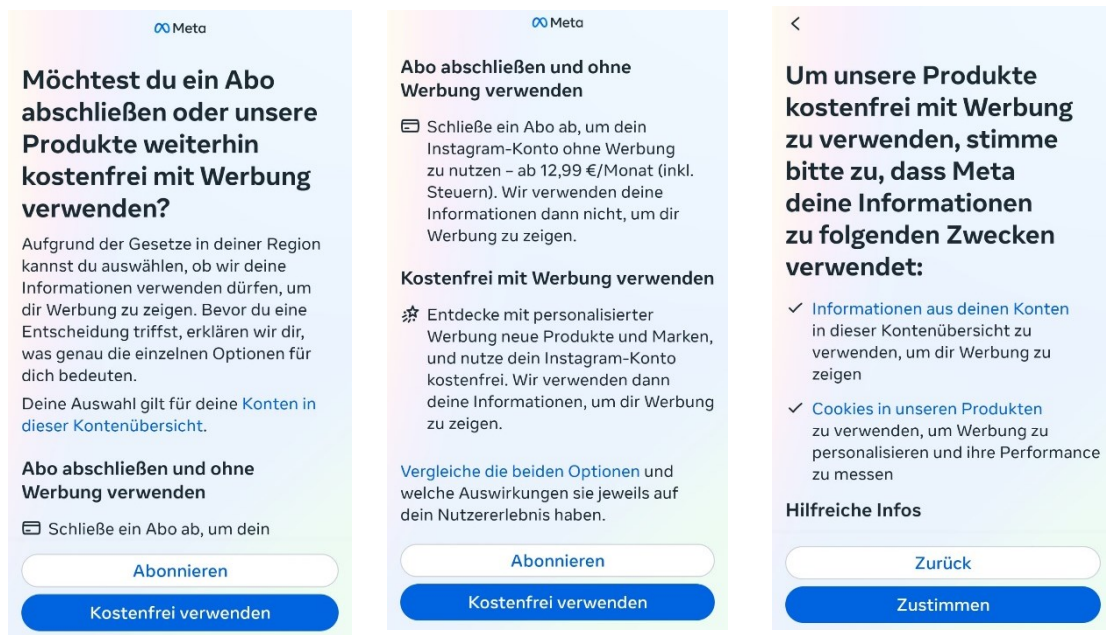


Figure 6 Meta subscription (Meta, 2024)

Because of the Digital Market Act, the Digital Service Act and the GDPR (General Data Protection Regulation), Meta has implemented a subscription option, to comply with the binding decision and the EU regulations. This option allows users to either pay for the services and not receive advertisements or use the platform, as stated “for free with advertisement” (see **Figure 6**) (Meta, 2023b).

In that regard, Meta highlights the following: *“We believe in an ad-supported internet, which gives people access to personalised products and services regardless of their economic status.”* (Meta, 2023b).

The outlined strategy of Meta illuminates the fact that the platform relies on personal data for profit, as the company is trying to avoid a complete ban on processing personal data for behavioural advertising. In view of this, the difference between agreeing to the terms and conditions or agreeing to use the platform without the subscription is hardly any different. The notion of “consent” must also be questioned, as the platform uses tracking technologies to generate and extract personal data, which the users are often not aware of. The platforms use

hidden technologies, such as cookies, pixels, and other technologies, which have been outlined in Chapter 6.1.4 to generate and extract personal data. The systematic way in which personal data is being generated and extracted by the platforms underlines that the monetisation of personal data describes the core mechanisms of the platform businesses.

Moreover, Meta's description of the use of the platform "for free, but with advertisement" highlights how the platform presents data to the public. The value of data is veiled by stating that the platform can be used for free, even though the users are "paying" with their data. Breidbach and Maglio (2020) have highlighted, that the "true" value of data is mostly veiled by the platforms because they need to ensure that data is generated, which they can use for profit (Breidbach & Maglio, 2020, p. 168).

Following Sadowski (2019) this aspect is of particular importance because data does not exist as a natural resource, which is freely available. Rather data is being manufactured (similar to digital risks). By suppressing this fact, the dimension of "regimes of data accumulation" can be reinforced (Sadowski, 2019, p. 2). Lupton (2020) has pointed out, that the term "data" implies a form of scientific neutrality, which enables a form of "dehumanisation". That is the case because personal data, which can describe intimate information about individuals is presented as "raw material" (Lupton, 2020, p. 45).

Furthermore, Zuboff (2019) claims in her book "The Age of Surveillance Capitalism", that the human experience has become raw material, which is translated into behavioural data. This data is evaluated by technology, such as artificial intelligence and algorithms, which make predictions about future behaviour. That is why Zuboff (2019) concludes, that the value of data is based on what she calls "behavioural surplus" (Zuboff, 2019, pp. 8–9). Also, Lupton (2020) has highlighted that personal data is attached to a form of "biovalue", which is exploited for profit (Lupton, 2020, p. 8). Following Mejias and Couldry (2019) this quantification of human life generates value in the platform economy (Mejias & Couldry, 2019, p. 3).

The process of monetising personal data has already been outlined and will only be revisited briefly. Personal data is generated and extracted by the platforms using technologies, which sometimes are not visible to the users. This data is then analysed based on predictive analysis, using algorithms, artificial intelligence, and deep machine learning, which enable the platforms to predict human behaviour and interests. The information extracted from the data is then used for personalised recommendations, which are distributed through algorithmic recommendation systems and content moderation. The personalised content includes advertisement, as the platform businesses can directly target its users, due to the detailed personal information they

possess, which makes the platforms valuable and profitable (Breidbach & Maglio, 2020, p. 164; Huhtala, 2019, p. 56; Siegel, 2013; Trzaskowski, 2022, p. 449; Zuboff, 2019, pp. 65–66).

This process of monetising data to target and influence users is also highlighted on TikTok's website for business, where TikTok promotes the platform to businesses by stating the following:

“- 81% of TikTok users who made a Back to School purchase said the platform played a role in purchases/gifts bought.

- TikTok users are 1.8x more likely to convince their family and friends to buy the item they purchased previously (vs. non-TikTok users).

-After viewing a Dynamic Showcase Ad on TikTok, 74% of Gen Z weekly TikTok users would seek more information on the advertised product.” (TikTok, 2022a).

The statements of TikTok highlight that the platform is valuable due to the influence TikTok has on its users. In this context, the already outlined technologies play a central role in influencing social media users and thus enable the platforms to generate profit (Fernández et al., 2021, p. 8; Pathak et al., 2023, p. 2). Due to the gatekeeper position of VLOPs, only a few businesses are in a position, in which they can decide what information is presented to the users. Given this, personalisation and the use of artificial intelligence and algorithms for content moderation are linked to power asymmetries, as the platforms can survey and manipulate their users for profit (Trzaskowski, 2022, pp. 449–450).

Jeon (2021) has conducted a case study analysis for the “Expert Group for the Observatory on the Online Platform Economy” of the European Commission on the advertisement practices of Google and concluded that the advertisement practices of the platforms lack in transparency and are linked to the market power of the platforms, which enable them to exploit personal data for profit by influencing the users of platform services. As most platform businesses function in a similar way the study highlights that businesses of the platform economy rely on monetising personal data for profit (see Jeon, 2021).

Particularly the technological architecture of the platform businesses highlights their drive for profit, as the rights and rules are set by the platforms and embedded in their architecture, which are enforced by the technology itself. For example, push notifications, which try to catch the user's attention are included in the default settings. Moreover, the platforms give incentives and nudge their users to click on ads or content (Saadatmand et al., 2019, pp. 1–2; Schneider, 2018, p. 134).

In view of this, the algorithmic recommendation systems play a key role in generating profit, as they are responsible for keeping the users engaged and for showing the users advertisements. The content curation and recommendation system are based on algorithms, which function based on artificial intelligence and thus automated decisions. As already outlined in Chapter 3 the technological systems, which are used by the platform businesses to generate profit, can be characterised by a lack of human involvement. This aspect was highlighted particularly in the context of TikTok's algorithm, which automatically ranks videos "weighted based on their value". Given this, the algorithm is programmed based on the economic logic of profit to decide what is valuable or not (Araujo et al., 2020, p. 611; Breidbach & Maglio, 2020, p. 173; TikTok, 2023b).

Particularly the use of those automated technologies for profit is linked to digital risks, as outlined in the previous chapters. The analysis of the risk of misinformation/ disinformation has highlighted how social media platforms enable the rapid spread of misinformation and disinformation. The reason for that is that the automated and personalised recommendation systems are programmed in a way, which keeps the users as engaged as possible, to generate data and make a profit out of the user's attention. That is why the algorithmic recommendation systems recommend content, which for example triggers strong emotions (Fernández et al., 2021, p. 8; Pathak et al., 2023, p. 2).

Bontridder and Poulet (2021) have stressed in their research on the role of AI in disinformation, that "the disinformation problem is mainly caused by the business model of the web that is based on advertising revenues, and that adapting this model would reduce the problem considerably" (Bontridder & Poulet, 2021, p. 1).

The academic research on automated systems and algorithmic recommendation systems suggests that the algorithms are programmed in a way, which focuses on generating profit. Therefore, content is recommended regardless of what effects it has on the users, as long as it keeps the user engaged and does not violate the community guidelines (Baptista et al., 2023, p. 2; Bontridder & Poulet, 2021, p. 5; Fernández et al., 2021, p. 2).

This aspect has particularly been highlighted by the analysis of the negative effects social media can have on user's physical and mental wellbeing. The research has shown that the recommendation system of TikTok and Instagram uses information on disorders, anxiety, or depression to recommend content, which triggers those aspects. That is the case because the algorithmic recommendation system uses personal information to predict interests and future behaviour. If a person has an eating disorder and is more likely to engage with content related

to the eating disorder, such as fitness videos, the algorithm will likely suggest that type of content, which can facilitate the eating disorder (Dondzilo et al., 2023, pp. 2–4). Moreover, also the specific targeting of teens and pre-teens (e.g. children) on TikTok has shown that the recommendation of personalised content goes along with risks for young adults. The reason for that is not only the potential inappropriate content that is suggested to young users but also that the algorithmic recommendation system is programmed in a way to make the platforms as addictive as possible. In that context, TikTok is an important example as the platform specifically targets teens and pre-teens (Pedrouzo & Krynski, 2023, p. 4; Zeng et al., 2021, p. 3162).

Moreover, the analysis of digital risks has also highlighted that personalised content is linked to the potential radicalisation of social media users, as the recommended content can reinforce and influence opinions, due to filter bubbles and echo chambers (Burton, 2023, p. 3). Particularly filter bubbles play a central role as Eli Pariser (2012) has argued. Filter bubbles are generated by technologies which reproduce the user's interests and behaviours (Pariser, 2012, pp. 14–15). Filter bubbles are produced by algorithms through personalisation, which is why users are likely to engage with content that represents already existing interests (Ross Arguedas et al., 2022, p. 11). Therefore, filter bubbles can be seen as a negative side effect of the algorithmic recommendation system, which is based on personalisation. Pathak et al. (2023) have outlined how filter bubbles can lead to radicalisation through a loop of misinformation (Pathak et al., 2023, p. 2).

Given this, the digital risks are not only facilitated by the algorithmic content moderation and recommendation systems but also linked to the general design of the social media platforms. The For You Page of TikTok and the Instagram feed are specifically designed in a way, which enables an easy engagement with the personalised content. Moreover, the full screen, which shows content and the swipe mechanism (see **Figures 3 and 4**) makes the platforms addictive, which is provoked by the economic logic of the data-driven business models. Those mechanisms enable a rapid consumption of short videos or images on the platforms, keeping the user engaged and satisfied (Saadatmand et al., 2019, p. 4; Zeng et al., 2021, p. 1363).

The problem of biased technological systems which facilitate discriminatory practices, has been outlined in the analytical part on digital risks. The algorithms are trained with human data, which can generate algorithmic bias. In view of this discriminatory practices are facilitated by the platforms by automatically removing content based on the biased algorithmic systems. The analysis of discrimination as a digital risk has highlighted that content is often removed or

flagged from racial or gendered minority groups based on algorithmic discrimination (Bouchardet, 2023; Haimson et al., 2021; Peterson-Salahuddin, 2022).

In addition, the outlined numbers on how much content is removed on TikTok and Instagram based on automated systems highlight the crucial role technology plays in the context of digital risks and their mitigation. Content moderation is mainly based on automated systems, which are linked to power dimensions of technology as they have structuring effects. That is the case as the automated technology used by the platforms determines what type of content is distributed to whom (Kenney et al., 2021, p. 1455).

Against this background, it must be underlined, that social media platforms are not necessarily using discriminatory practices on purpose. Rather they use deep learning mechanisms and artificial intelligence, which is trained with human data. This can reproduce human bias as the algorithms are coded in a way, which generates probabilities as an output (Agan et al., 2023, p. 2; Breidbach & Maglio, 2020, p. 173; Prinzing, 2019, p. 271). In that regard, it is unclear what concrete data sets TikTok and Instagram use to train their algorithms.

Pasquale (2015) has underlined in his book “the black box society”, that society is faced with a knowledge problem, due to the functioning of algorithms being non-transparent and complex, which is why they cannot be understood by the public. This is linked to the profit-driven interests of platform businesses, as they keep the information on their algorithmic systems veiled, which enables them to be in a powerful position, due to the knowledge asymmetry concerning the technology used (Pasquale, 2015). Also, Pathak et al. (2023) pointed out, that for example in the context of misinformation the current research lacks an understanding of how the algorithmic recommendation systems function and impact the spread of misinformation on social media (Pathak et al., 2023, p. 2). This highlights that also academic research is affected by the lack of information regarding the technological systems used, which this thesis is also affected by, as the information gathered on TikTok and Instagram's website do not give any detailed information on how the algorithms function.

Amoore (2020) understands the logic of algorithms to be “*an arrangement of propositions that significantly generates what matters in the world.*” (Amoore, 2020, p. 26). The outlined technologies of social media businesses, are affecting the way reality is perceived by its users (Bontridder & Pouillet, 2021, pp. 4–5). Against this background van Dijck et al. (2018) have underlined, that particularly social media platforms are never neutral digital services. The platform mechanisms, such as algorithmic filtering decide what is made visible and what not

(José van Dijck et al., 2018, p. 32). This aspect is particularly important, as it highlights the relevance of algorithms in the context of the digital risk society.

Thus, the conducted analysis has highlighted that the focus on monetising personal data for profit, through the use of automated technologies, is linked to digital risks for society by prioritising profit over social implications (Peterson-Salahuddin, 2022, p. 6; Wahid, 2023, p. 108). This can be linked back to the Digital Service Act, which has outlined the following factors that may influence systematic risks and should be considered for the obligatory risk assessment for VLOPs (article 34 no. 2):

- “(a) the design of their **recommender systems** and any other relevant **algorithmic system**;*
- (b) their content moderation systems;*
- (c) the applicable **terms and conditions** and their enforcement;*
- (d) systems for selecting and presenting **advertisements**;*
- (e) **data-related practices** of the provider.”* (European Union, 2022, p. 64).

The previous analysis has shown that the factors that may influence systematic risks outlined in the DSA are congruent with the outlined technologies and practices used for profit. Given this, the factors described in the DSA represent the mechanisms platform businesses use to monetise personal data and are thus the factors which the platform businesses rely on to generate profit. Particularly the technological systems, such as the algorithmic recommendation system and the personalisation processes, represent essential components of the data-driven platform businesses and their economic logic. As shown those practices are deeply interwoven with the digital risks, which is why the previous analysis of digital risks posed by social media platforms has highlighted that digital risks are interwoven with the technologies used by the platforms. Those technologies are needed to generate profit, as outlined above, which would speak in favour of the hypothesis, that *digital risks may represent a prerequisite for the platform economy because some of the systematic risks identified by the DSA are deeply intertwined with the way profit is generated by VLOPs.*

This is particularly relevant in the context of the mitigation measures outlined in the DSA (see Chapter 4.2.3), such as adapting the terms and conditions, the content moderation process, the algorithmic system/recommendation system and adapting the advertisement procedures (European Union, 2022, p. 65). The results of the case study analysis would imply that if platforms would try to properly manage and mitigate the digital risks which arise out of their services, they would have to damage their business model. That is the case because the

platforms would need to rethink how they use their technology and how they monetise data, as the digital risks arise out of their drive for profit. That is why the role that the EU assigned private businesses in the DSA through the risk-based approach must be questioned. This will be discussed in more detail in the following chapter.

To conclude, the analysis in this thesis has shown that platform businesses use technology to monetise personal data. The case study analysis of TikTok and Instagram can be linked back to the general logic of the platform economy, as the two chosen cases are representative of the general logic of the data-driven business model in the platform economy. The analysis has shown that the use of automated technologies goes along with digital risks, as the technologies are mainly used in a way to generate profit, irrespective of the negative effects on society and individuals. The analysis has shown that digital risks arise as a “negative side effect” out of the economic logic of platform businesses. This is a crucial aspect as private businesses have become relevant actors in the public sphere of the digital risk society. That is particularly the case in the context of the DSA, as the European Union has assigned platform businesses a crucial role in the context of risk regulation for society. The implications in the context of the DSA and the digital risk society will be discussed in the following part.

7. Discussion: Platforms as the new digital risk evaluators in the Digital Risk Society?

The analysis of digital risks posed to society, which arise out of data-driven platforms has highlighted the crucial role platform businesses play for society. Moreover, the analysis has shown that the European Union has assigned private platforms the role of digital risk regulators through the Digital Service Act. That is the case because VLOPs are obligated to identify, analyse and assess systematic risks stemming from their services and develop strategies to mitigate those risks (European Union, 2022, p. 64). As already outlined the DSA does not give any information on how the risk assessment has to be conducted by the platforms and how the systematic risks have to be identified (Loi, 2023, pp. 2–3). This assigns private businesses the role of developing the risk assessment which makes them responsible for creating tools and approaches to identify digital risks, leaving them a wide room for interpreting and defining digital risks (Barata, 2021, p. 3). Given that Peukert (2021) has pointed out that this aspect is crucial, as important decisions are left up to the VLOPs, which can also lead to grey areas through which the platforms could circumvent the regulation (Peukert, 2021, p. 23).

This is of particular importance as the EU not only also assigned private businesses a crucial role in the negotiation process around digital risks.

In that regard Beck (2008) has highlighted that the definition of the term risks is to be seen as an ongoing discourse in the (digital) risk society, highlighting that (digital) risks are a social construct and are therefore subject to negotiations (Beck, 2008, p. 66). The Digital Service Act indicates a negotiation of digital risks, in which platform businesses themselves play a significant role. The reason for that is that the DSA is grounded on a risk-based approach, for which VLOPS are obligated to perform a risk assessment, in which they have to define, identify and measure the digital risks, which affects the way digital risks are perceived (Gregorio & Dunn, 2022, pp. 2–3). Given this, it must be questioned why the EU assigns private businesses this role, as they have a clear economic interest and are private actors operating in the public sphere.

This aspect is linked to power and knowledge asymmetries, which are important to highlight as the DSA assigns the private businesses with the role of protecting society from future risks, through the risk-based approach. Revisiting the outlined work on digital risks Beck (2014) highlighted that the “anticipation of the catastrophe itself” is what becomes important in the context of digital risks because it is the only way, in which a space to counter those risks can open up (Beck, 2014). If the private platform businesses are entrusted with the role of risk regulators, they become the ones in power of being able to “anticipate” the digital risks, because they are the only actors which fully understand the digital risks, as they are posed by their systems. Because of this, the DSA relies on information given by private businesses, which highlights the powerful role the DSA assigned the platforms. Given this, it is questionable to what extent the platform businesses are able and willing to sufficiently provide information on the digital risks and manage them, as the digital risks are deeply interwoven with the economic logic of their business models.

Furthermore, the due diligence obligations for VLOPs highlight that the EU focuses on underlining the accountability and responsibility of platform businesses in the context of digital risks. This shifts the governmental responsibility of protecting society through regulating digital risks towards the private businesses (Gregorio & Dunn, 2022, pp. 2–3). This must be questioned, especially considering the results of the case study analysis, which has revealed that the digital risks, which arise out of the platforms can be linked back to the way the platform businesses monetise personal data for profit. Therefore, the digital risks are manufactured and thus based on the actions and decisions of the platforms (Bonß, 2022, p. 6). The case study analysis has shown that, if the platforms would regulate their risks, as outlined in the DSA, particularly in the mitigation measures, they would eventually have to damage their business, as the digital risks are an essential component of their economic logic. This aspect highlights

the potential different and contrary interests of the private actors in the context of regulating digital risks, which is why the DSA contains a conflict of interests.

The self-presentation of the private businesses is particularly interesting, as they present themselves to the public as not being businesses, but rather as essential to society, which foster technological and economic innovation, enable communication and communities and can be seen as trusted partners for governments (Meta, 2024; TikTok, 2023e).

Meta for example states the following in regard to its mission: *“We research for the good of people around the world, like to advance technology or to help out in a crisis.”* (Meta, 2023a).

Against this background, it must be underlined that the outlined academic definitions of social media in Chapter 6.1.1 employ a similar perspective of (social media) platforms to the self-perception of the businesses, which is why it must be questioned if academic research is reproducing the hidden economic logic of platform businesses, through the way platforms are perceived and defined in academia. Therefore, academic research is duplicating the self-image of the platform businesses, instead of questioning it critically.

Furthermore, the case study analysis (Chapter 6), which has revealed that the platform businesses present themselves mostly through being driving forces for innovation, can be linked to a notion of “technological determinism”. That is the case, because the platforms present their services, as highlighted by Meta’s (2023a) statement above, with innovation and services for society, through technology. In the digital risk analysis, it was highlighted, that the platforms have recognised the digital risks their services may pose to society. Given this, they present themselves as responsible actors, which implement strategies to ensure their users are safe and protected. This image management veils the essential role, which the platforms and their technologies play in manufacturing digital risks. That is particularly the case in the context of the control and ownership over personal data (Beck, 2017, p. 87-88, 189).

In view of this, the case study analysis has outlined how platforms present their business with personal data, by describing personal data as raw material, which is available as a “natural resource” and thus can be used for profit. Moreover, this thesis also highlighted how platform businesses veil the value of data to their users, by using the term “information” instead of “data” in their policies, which implies that the information is already available and just collected and used by the platforms. This veils the fact that hidden tracking technologies are used to not only extract but also generate personal data, which are processed into personal information and are thus not “naturally existing” (Breidbach & Maglio, 2020, p. 168; Lupton, 2020, p. 45; Sadowski, 2019, p. 2).

Even though they are also relevant in this context, the debates around data and information have only been touched upon briefly. From the author's point of view, on the one side data can be seen as raw material, which is processed into information about its users and thus valuable for private businesses. On the other side, debates focus on information, which only becomes valuable in the context they are getting used in. This aspect needs to be further researched, highlighting debates around how data is getting used, for what purpose, why it is owned by private businesses, what that means for society and what potential alternative (non-exploitative) ways of data ownership could be.

The DSA does not address problems that arise out of the ownership of personal data by private businesses, even though it is a key factor in the context of digital risks. The DSA does not question the business model of the platforms, which would be essential in the context of regulating digital risks. That is the case because digital risks arise out of the way personal data is monetised, which is why the technological systems, from which the digital risks stem, are solely used to generate profit. This process must be seen critically, which is why the personal data ownership of private businesses, and the way personal data is currently monetised must be questioned.

Furthermore, not only the ownership of personal data by private businesses is problematic, but also the "ownership" of the knowledge around the technologies used for monetising data is linked to power asymmetries, which has been outlined briefly in this discussion. Particularly, the elaborations on the digital risk society, in which knowledge about technology plays a key role, as it is linked to decision-making power, highlights the role of platform businesses in the context of the DSA (Sundberg, 2023, p. 3). In view of this, Giddens (1999) has highlighted that technology is particularly dangerous, due to the lack of fully understanding the technology, which is why „technological frontiers“ are generated (Giddens, 1999, p. 3). The analysis of digital risks has shown that the lack of knowledge of the technological systems employed by private businesses, such as automated algorithmic systems, leads to a limited ability in fully understanding digital risks, particularly for academia (Dutt, 2023, p. 357).

This is also provoked by the platform businesses as they do not give any detailed information on their systems used. The DSA could enable a better understanding of the digital risks, as VLOPs are obligated to share data with researchers, which enables them to conduct research related to the detection and understanding of digital risks (Husovec & Roche Laguna, 2022, p. 10; Turillazzi et al., 2023, p. 87). Nevertheless, the outlined key characteristics of digital risks have underlined that the public is dependent on experts and the platforms themselves, to

understand the logic of their systems and the digital risks linked to those systems (Beck, 2017, p. 186). Against this background, platforms can only be regulated democratically if their complex key mechanism is understood (Poell et al., 2019, p. 9).

Furthermore, to regulate digital risks, they do not only have to be understood properly but also the implementation of mitigation measures must be controlled. That is why, the goal of the regulation is not to eliminate the digital risks, but to reduce them to an “acceptable level”, enabling more control over the risks (Gregorio & Dunn, 2022, pp. 2–3). The DSA outsources the application and enforcement of the regulation to private entities, such as third-party auditors (Cauffmann & Goanta, 2021, p. 768). This must be seen critically, as private auditors are mostly profit-based and may have contradictory interests (Cauffmann & Goanta, 2021, p. 771). Moreover, the technologies used for analysing risks and developing mitigation measures, often fail to address digital risks sufficiently, because they fail to take into consideration, that they are socially constructed, by only focusing on probabilities and numbers (Aven, 2012, p. 1044; Lupton, 2023, pp. 25–26; Rosa, 2003, p. 72). This aspect is particularly concerning, because the knowledge around digital risks, especially from a governmental perspective is informed by the risk assessment and what methods, tools and approaches are being used to analyse digital risks (Rosa et al., 2015, p. 77).

Overall, the specific obligations and mitigation measures for VLOPs highlight, that the DSA characterises filtering, sorting, and optimising content as a purely technical and passive role, which does not acknowledge the profit-oriented drive of online platforms. This is problematic because it does not equate to the profit-oriented and technologically-driven world that society is already faced with and continuous to develop (Buiten, 2021, p. 379).

Against this background, it is unclear how the EU exactly conceptualises the platform businesses. The DSA recognises that VLOPs have the power to influence information, opinions and ideas. This highlights that VLOPs play a critical role in the context of facilitating public debates, economic transactions, and the dissemination of information (European Union, 2022, p. 21). The DSA highlights the essential role platforms play in society, which could be linked to the perspective of platforms representing a kind of infrastructure to society. On the other side, the DSA is part of the strategy package of the EU which includes the Digital Markets Act (DMA). In the DMA platform businesses are introduced as “gatekeepers” of digital markets (European Commission, 2023a). Considering this, the different perspective on platforms goes along with different implications. If platforms are introduced as digital infrastructure, they are linked to public elements, which would question the private ownership of the infrastructure, as

it is essential to society. If platforms are seen as marketplaces, this would be linked to an economic logic of exclusivity, which could legitimise the private ownership of data, as private businesses are providing services in a competitive sphere, which is why the economic logic of profit becomes the driving force. In that regard, it is unclear why the EU assigns private businesses the role of risk regulators for society, without recognising them as services which provide essential infrastructure. The understanding of platforms as services could be linked to the connotation of marketplaces, which is why the regulation of digital risks should not be conducted by the private businesses but rather must be undertaken by public institutions.

Concluding, the discussion has illuminated, that the EU has assigned platform businesses a crucial role in regulating digital risks posed to society. The DSA shifts the responsibilities of regulating digital risks from the EU to the private platform businesses. In this sense, platforms become private actors, which operate in the public sphere. This can be linked back to the elaborations on the digital risk society, which highlights that “digital modernity” can be characterised by an overlap of the state, individuals, and the private economy (Beck, 2017, p. 193). Taking this into account, it is questionable to what extent private businesses are able and willing to regulate digital risks stemming from their services, as the digital risks represent an essential component of the economic logic of the data-driven platform businesses.

8. Conclusion

In summary, this thesis has critically examined the Digital Service Act of the European Union, through employing an interdisciplinary perspective on the economic logic of platform businesses and the digital risks which are stemming from their services.

The DSA can be described as the first attempt to regulate platform businesses on an international level. The EU has acknowledged that digital platforms have become an essential part of individuals' lives, which pose risks to society. Given this, the EU has outlined systematic risks for Very Large Online Platforms, which arise out of their services and factors that may influence those risks, such as the algorithmic recommendation system or the automated content moderation (see European Union, 2022). The regulation is grounded on a risk-based approach, which obligates VLOPs to conduct a risk assessment and develop mitigation measures for the digital risks stemming from their services. The DSA focuses on reinforcing the responsibility and accountability of private businesses, through imposing due diligence obligations on them.

This thesis critically examined VLOPs by illustrating how the digital risks outlined in the DSA are deeply interwoven with the economic logic of the data-driven platform businesses. The case study analysis of TikTok and Instagram has revealed that the digital risks of

misinformation/disinformation, negative effects on mental/physical wellbeing, negative effects on children/young adults and discrimination/bias are linked to the business models of the services. Particularly the personalisation process and linked to this the algorithmic recommendation system and automated content moderation, have been shown to generate and reinforce digital risks. That is the case because the monetisation of personal data is the driving force of businesses, which is why technological systems are mainly employed for profit-oriented purposes irrespective of the negative effects on society and individuals. In view of this, hidden technologies are used to generate and extract personal data, which is processed by automated systems that are programmed to directly target users with personalised content and advertisement. Moreover, TikTok and Instagram have been shown to design their interfaces in a way which is highly addictive and keeps users as engaged as possible, this is particularly dangerous for children and young adults, as they are the main target group of social media platforms. Given this, it was outlined how algorithms are programmed to recommend personalised content, which triggers strong emotions in users. This reinforces the distribution of misinformation and can lead to the recommendation of potentially harmful content to users with physical or mental health problems. Furthermore, the case study analysis has revealed discriminatory practices of the platforms, due to biased algorithms, which are used to automatically remove or flag content.

Consequently, the results of the case study analysis have revealed that digital risks arise as a “negative side effect” out of the economic logic of platform businesses. TikTok and Instagram can be characterised as representative platform businesses, which highlight the general practices and logic of data-driven business models of the platform economy. In that sense, this thesis concludes that digital risks may represent a prerequisite for the platform economy because some of the systematic risks identified by the DSA are deeply intertwined with the way VLOPs generate profit.

From this point of view, it is questionable to what extent private businesses are able or willing to regulate digital risks, as the digital risks seem to represent an essential component of their business model. Given this, platforms would have to damage their business model, if they would sufficiently address the due diligence obligations imposed on them by the DSA, which is why the DSA contains a conflict of interests. Hence, the role of digital risk regulators, which the EU has assigned to private businesses must be seen critically. The DSA reproduces the image management of the private businesses, which assign themselves an essential role and responsibility for society, veiling their contradictory economic interests. The DSA fails to

question the profit-oriented mechanisms of the platform businesses, which undermines the role platform businesses play in manufacturing digital risks.

Platform businesses become important actors in defining digital risks, as the identification and assessment of digital risks are based on the information, they are willing to share. This aspect was highlighted in the outlined research around digital risks, as the knowledge around the algorithmic recommendation and content moderation systems is still limited, due to a lack of transparency. Therefore, digital risks are veiled and linked to power and knowledge asymmetries. This aspect is particularly important in the context of the DSA, as the understanding of digital risks mainly relies on expert knowledge and the information, which the platforms provide in their risk assessments. That is why it is crucial to critically investigate the obligatory risk assessment and mitigation measures of the platforms, which will be submitted to the EU. Hence, this thesis has outlined potential issues regarding the sufficient implementation of the DSA, which underlines that future research is needed particularly regarding the technological systems, which are used for profit.

Against this background, it must be underlined that the research on digital risks is still limited. This thesis is faced with limitations as it lacks empirical evidence. Particularly limitations considering the conducted case study analysis must be outlined. The digital risk analysis has only given an overview of studies related to digital risks. Each digital risk outlined could have been subject to an independent thesis, which highlights that the analysis does not do justice in deeply understanding and studying each digital risk. Rather the purpose of this thesis was to illustrate digital risks in the light of the research question.

This thesis has not provided an extensive analysis of the academic definitions of platforms, but rather an overview of commonly cited definitions was given. In view of this, it is important to highlight the role academia plays in duplicating the self-image of private businesses, which needs to be further researched.

Furthermore, the debates around interactions (human-human, human-machine, machine-machine) and digital social inequalities were not included in this thesis, due to the already wide scope of the research question. Nevertheless, those aspects are important to take into consideration when researching digital risks.

Additionally, the development of timelier definitions and concepts around digital risks and the digital risks society is needed, for which this thesis contributed by outlining the emerging research around of digital risks, society and regulations. In this regard particularly by revisiting traditional workaround risks and the risk society can assist in further developing the concept of

the digital risk society, as meaningful insights into the hidden logic of digital risks and their power dimensions can be drawn from it. In that regard it has been highlighted, that the work around digital risk is conducted within single academic disciplines, but rarely in an interdisciplinary manner, which is urgently needed to fully understand the current developments. Moreover, the (digital) risk society fails to give attention to how risks are experienced and discussed in countries of the Global South, which is why perspectives and research from the Global South need to be included.

Given this it must be highlighted that the purpose of this thesis was by no means, to characterise platforms as services which only have negative effects on society nor was the purpose to state that the DSA does not have any positive implications. Rather the focus was on highlighting potential challenges which can arise out of the economic logic of platform businesses for the implementation of the DSA. It was highlighted that the EU has introduced a crucial and urgently needed regulation for digital services. Particularly the obligations for platform businesses to become more transparent about their economic practices are important changes, which challenge the platform businesses and strengthen user's agency. This thesis has contributed to the research on digital risks and their regulation by outlining factors, which have implications for the implementation of the DSA and thus need to be taken into consideration.

The DSA obligates VLOPs to share information and data with researchers in order to facilitate the detection and understanding of digital risks stemming from their services. This thesis has outlined some relevant research gaps regarding the automated algorithmic systems and the understanding of the economic logic of the platform businesses, which indicates future research directions.

Concluding it was highlighted that the DSA shifts the responsibilities of regulating digital risks towards private businesses, which are assigned the role of digital risk regulators. This must be seen critically as private platforms become crucial and powerful actors in the public sphere. That is why, it is questionable to what extent private businesses are able and willing to regulate digital risks stemming from their services, as digital risks represent an essential component of the economic logic of the data-driven platform businesses. Particularly the private ownership and monetisation of personal data must be questioned and included in debates around digital risk regulations. In this sense it is important, to highlight the conflicting economic interests of private businesses in the context of the DSA, to prevent the regulation from becoming a "toothless tiger". That is why the EU should not shift the responsibility of regulating digital risks towards private businesses by relying on their conducted risk assessments. Finally, the

DSA can be seen as a first step in the right direction, paving the way towards a better understanding of digital risks and their implications. In light of this, the regulation of private businesses is crucial to protect society and democracy from digital risks and their harmful consequences.

9. References

- Acs, Z. J., Song, A. K., Szerb, L., Audretsch, D. B., & Komlósi, É. (2021). The evolution of the global digital platform economy: 1971–2021. *Small Business Economics*, 57(4), 1629–1659. <https://doi.org/10.1007/s11187-021-00561-x>
- Agan, A., Davenport, D., Ludwig, J., & Mullainathan, S. (2023). *Automating Automaticity: How the Context of Human Choice Affects the Extent of Algorithmic Bias*. Cambridge, MA: National Bureau of Economic Research. <https://doi.org/10.3386/w30981>
- Alemanno, A. (2016). Risk and Regulation. In A. Burgess, A. Alemanno, & J. Zinn (Eds.), *Routledge Handbook of Risk Studies* (pp. 191–203). Abingdon, Oxon, New York, NY: Routledge, 2016.: Routledge.
- Alemanno, A., Butter, F. den, Nijsen, A., & Torriti, J. (2016). Introduction. In A. Burgess, A. Alemanno, & J. Zinn (Eds.), *Routledge Handbook of Risk Studies*. Abingdon, Oxon, New York, NY: Routledge, 2016.: Routledge. Retrieved from 1-14.
- Amoore, L. (2020). *Cloud ethics: Algorithms and the attributes of ourselves and others*. Durham: Duke University Press. <https://doi.org/10.1515/9781478009276>
- Araujo, T., Helberger, N., Kruikemeier, S., & Vreese, C. H. de (2020). In AI we trust? Perceptions about automated decision-making by artificial intelligence. *AI & SOCIETY*, 35(3), 611–623. <https://doi.org/10.1007/s00146-019-00931-w>
- Are, C. (2020). How Instagram’s algorithm is censoring women and vulnerable users but helping online abusers. *Feminist Media Studies*, 20(5), 741–744. <https://doi.org/10.1080/14680777.2020.1783805>
- Aven, T. (2012). On the critique of Beck’s view on risk and risk analysis. *Safety Science*, 50(4), 1043–1048. <https://doi.org/10.1016/j.ssci.2011.12.004>
- Aven, T., & Renn, O. (2009). On risk defined as an event where the outcome is uncertain. *Journal of Risk Research*, 12(1), 1–11. <https://doi.org/10.1080/13669870802488883>
- Ayalde, J., Ta, D., Adesanya, O., Mandzufas, J., Lombardi, K., & Trapp, G. (2023). Awake and Alert: Examining the Portrayal of Energy Drinks on TikTok. *The Journal of Adolescent Health : Official Publication of the Society for Adolescent Medicine*, 72(4), 633–635. <https://doi.org/10.1016/j.jadohealth.2022.10.025>
- Azkan, C., Spiekermann, M., & Goecke, H. (2019). Uncovering Research Streams in the Data Economy Using Text Mining Algorithms. *Technology Innovation Management Review*, 9(11), 62–74. <https://doi.org/10.22215/timreview/1284>
- Baghdadi, J. D., Coffey, K. C., Belcher, R., Frisbie, J., Hassan, N., Sim, D., & Malik, R. D. (2023). #coronavirus on TikTok: User engagement with misinformation as a potential threat to public health behavior. *JAMIA Open*, 6(1), ooad013. <https://doi.org/10.1093/jamiaopen/ooad013>
- Bahnweg, E., & Omar, H. (2023). Effects of TikTok on Adolescent Mental Health and Wellbeing. *Dynamics of Human Health*, 10(1), 1–7.
- Baptista, J. P., Rivas-de-Roca, R., Gradim, A., & Loureiro, M. (2023). The Disinformation Reaction to the Russia–Ukraine War. *KOME*, 11(2). <https://doi.org/10.17646/KOME.of.2>
- Barata, J. (2021). *The Digital Services Act and the Reproduction of Old Confusions*. Fachinformationsdienst für internationale und interdisziplinäre Rechtsforschung. <https://doi.org/10.17176/20210302-154101-0>

- Bechmann, A., & Bowker, G. C. (2019). Unsupervised by any other name: Hidden layers of knowledge production in artificial intelligence on social media. *Big Data & Society*, 6(1), 205395171881956. <https://doi.org/10.1177/2053951718819569>
- Beck, U. (1992 (first 1986)). *Risk society: Towards a new modernity*. London: Sage Publications.
- Beck, U. (1999). Weltrisikogesellschaft, ökologische Krise und Technologiepolitik. In U. Beck, M. A. Hajer, & S. Kesselring (Eds.), *Der unscharfe Ort der Politik: Empirische Fallstudien zur Theorie der reflexiven Modernisierung* (pp. 307–334). Wiesbaden: VS Verlag für Sozialwissenschaften; Imprint.
- Beck, U. (2008). *Weltrisikogesellschaft: Auf der Suche nach der verlorenen Sicherheit* (1. Aufl.). Suhrkamp Taschenbuch: Vol. 4038. Frankfurt: Suhrkamp.
- Beck, U. (2014). Digital risk in the modern society. Retrieved from <https://www.socialeurope.eu/digital-risk>, [2023-10-16].
- Beck, U. (2017). *Die Metamorphose der Welt* (F. Jakubzik, Trans.) (2. Auflage). Berlin: Suhrkamp.
- Belk, R. (2014). You are what you can access: Sharing and collaborative consumption online. *Journal of Business Research*, 67(8), 1595–1600. <https://doi.org/10.1016/j.jbusres.2013.10.001>
- Benzie, A., & Montasari, R. (2022). Artificial Intelligence and the Spread of Mis- and Disinformation. In R. Montasari (Ed.), *Artificial Intelligence and National Security* (1st ed., pp. 1–18). Cham: Springer International Publishing; Springer. https://doi.org/10.1007/978-3-031-06709-9_1
- Bessi, A., & Ferrara, E. (2016). Social bots distort the 2016 U.S. Presidential election online discussion. *First Monday*. Advance online publication. <https://doi.org/10.5210/fm.v21i11.7090>
- Body of European Regulators for Electronic Communications (2019). *BEREC Report on the Data Economy*. Retrieved from <https://www.berec.europa.eu/en/document-categories/berec/reports/berec-report-on-the-data-economy>.
- Boffone, T. (2022). *Tiktok cultures in the United States*. London: Routledge. <https://doi.org/10.4324/9781003280705>
- Bonß, W. (2022). Von magischen Praktiken zu systemischen Risiken: Geschichte und Bedeutung des Risikobegriffs. *Aus Politik Und Zeitgeschichte*, 72(23-25), 4–11. Retrieved from <https://www.bpb.de/shop/zeitschriften/apuz/risikokompetenz-2022/508882/von-magischen-praktiken-zu-systemischen-risiken/>.
- Bontridder, N., & Pouillet, Y. (2021). The role of artificial intelligence in disinformation. *Data & Policy*, 3. <https://doi.org/10.1017/dap.2021.20>
- Börner, S. (2022). Social Policy and Solidarity. In S. M. Büttner, M. Eig Müller, & S. Worschech (Eds.), *Sozialwissenschaftliche Einführungen: Vol. 3. Sociology of Europeanization* (pp. 237–257). München, Wien: De Gruyter Oldenbourg.
- Botero Arcila, B., & Griffin, R. (2023). Social media platforms and challenges for democracy, rule of law and fundamental rights. Retrieved from [https://www.europarl.europa.eu/RegData/etudes/STUD/2023/743400/IPOL_STU\(2023\)743400_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2023/743400/IPOL_STU(2023)743400_EN.pdf), [2023-12-15].

- Bouchardet, C. (2023). The Colors of Content Moderation: A Portfolio of Brazilian Resistances to Coloniality on Instagram. *International Critical Thought*, 1–16. <https://doi.org/10.1080/21598282.2023.2296178>
- Bovet, A., & Makse, H. A. (2019). Influence of fake news in Twitter during the 2016 US presidential election. *Nature Communications*, 10(1), 7. <https://doi.org/10.1038/s41467-018-07761-2>
- Boyer, R. (2022). Platform capitalism: a socio-economic analysis. *Socio-Economic Review*, 20(4), 1857–1879. <https://doi.org/10.1093/ser/mwaa055>
- Breidbach, C. F., & Maglio, P. (2020). Accountable algorithms? The ethical implications of data-driven business models. *Journal of Service Management*, 31(2), 163–185. <https://doi.org/10.1108/JOSM-03-2019-0073>
- Brennen, J. S., & Kreiss, D. (2016). Digitalization. In K. Bruhn Jensen & R. T. Craig (Eds.), *The international encyclopedia of communication theory and philosophy: E-L* (pp. 1–11). Chichester, UK, Hoboken, NJ: John Wiley & Sons. <https://doi.org/10.1002/9781118766804.wbiect111>
- Bründl, S., Matt, C., & Hess, T. (2016). Daten als Geschäft — Rollen und Wertschöpfungsstrukturen im deutschen Markt für persönliche Daten. *Wirtschaftsinformatik & Management*, 8(6), 66–71. <https://doi.org/10.1007/s35764-016-0124-5>
- Buiten, M. C. (2021). The Digital Services Act From Intermediary Liability to Platform Regulation. *JIPITEC*, 12(5), 361–380.
- Burgess, J., Marwick, A., & Poell, T. (2018). Editors' Introduction. In J. Burgess, A. Marwick, & T. Poell (Eds.), *The SAGE Handbook of Social Media* (pp. 1–11). 1 Oliver's Yard, 55 City Road London EC1Y 1SP: SAGE Publications Ltd.
- Burton, J. (2023). Algorithmic extremism? The securitization of artificial intelligence (AI) and its impact on radicalism, polarization and political violence. *Technology in Society*, 75, 102262. <https://doi.org/10.1016/j.techsoc.2023.102262>
- Busch, C., Graef, I., Hofmann, J., & Gawer, A. (2021). *Uncovering blindspots in the policy debate on platform power: Final Report: Expert Group for the Observatory on the Online Platform Economy*. Retrieved from <https://platformobservatory.eu/app/uploads/2021/03/05Platformpower.pdf>.
- Campbell, S., & Currie, G. (2006). Against Beck. *Philosophy of the Social Sciences*, 36(2), 149–172. <https://doi.org/10.1177/0048393106287209>
- Cauffmann, C., & Goanta, C. (2021). A New Order: The Digital Services Act and Consumer Protection. *European Journal of Risk Regulation*, 12(4), 758–774. <https://doi.org/10.1017/err.2021.8>
- Ceylan, G., Anderson, I. A., & Wood, W. (2023). Sharing of misinformation is habitual, not just lazy or biased. *Proceedings of the National Academy of Sciences of the United States of America*, 120(4), e2216614120. <https://doi.org/10.1073/pnas.2216614120>
- Chatzopoulou, E., Filieri, R., & Dogruyol, S. A. (2020). Instagram and body image: Motivation to conform to the “Instabod” and consequences on young male wellbeing. *Journal of Consumer Affairs*, 54(4), 1270–1297. <https://doi.org/10.1111/joca.12329>
- Chen, L., Li, S., Wei, J., & Yang, Y. (2022). Externalization in the platform economy: Social platforms and institutions. *Journal of International Business Studies*, 53(8), 1805–1816. <https://doi.org/10.1057/s41267-022-00506-w>

- Chiarella, M. L. (2022). Digital Markets Act (DMA) and Digital Services Act (DSA): New Rules for the EU Digital Environment. *Athens Journal of Law*, 9(1), 33–58. <https://doi.org/10.30958/ajl.9-1-2>
- Clegg, N. (2023). How AI Influences What You See on Facebook and Instagram. Retrieved from <https://about.fb.com/news/2023/06/how-ai-ranks-content-on-facebook-and-instagram/>, [2023-12-24].
- Corcos, A., & Hodara, L. (2023). How social media are collecting more of users' data: a behavioral model of platform retention strategies. *SN Business & Economics*, 3(7). <https://doi.org/10.1007/s43546-023-00501-9>
- Council of Europe (2024). Hate speech and violence. Retrieved from <https://www.coe.int/en/web/european-commission-against-racism-and-intolerance/hate-speech-and-violence/>, [2024-01-11].
- Council of the European Union (2023). Infographic- The EU's platform economy. Retrieved from <https://www.consilium.europa.eu/en/infographics/platform-economy/>, [2023-11-28].
- Curran, D. (2013). Risk society and the distribution of bads: Theorizing class in the risk society. *The British Journal of Sociology*, 64(1), 44–62. <https://doi.org/10.1111/1468-4446.12004>
- Curran, D. (2016). Risk Society and Systematic Social Theory. In D. Curran (Ed.), *Risk, Power, and Inequality in the 21st Century* (pp. 42–62). London: Palgrave Macmillan UK. https://doi.org/10.1057/9781137495570_3
- Curran, D. (2018). Risk, innovation, and democracy in the digital economy. *European Journal of Social Theory*, 21(2), 207–226. <https://doi.org/10.1177/1368431017710907>
- Danermark, B. (2019). Applied interdisciplinary research: a critical realist perspective. *Journal of Critical Realism*, 18(4), 368–382. <https://doi.org/10.1080/14767430.2019.1644983>
- Data Protection Commission (2023). Irish Data Protection Commission announces €345 million fine of TikTok. Retrieved from <https://www.dataprotection.ie/en/news-media/press-releases/DPC-announces-345-million-euro-fine-of-TikTok>, [2024-01-10].
- Daum, T. (2019). *Das Kapital sind wir: Zur Kritik der digitalen Ökonomie* (3. Auflage). Nautilus Flugschrift. Hamburg: Edition Nautilus.
- Decarolis, F., & Li, M. (2023). Regulating online search in the EU: From the android case to the digital markets act and digital services act. *International Journal of Industrial Organization*, 90, 102983. <https://doi.org/10.1016/j.ijindorg.2023.102983>
- Dondzilo, L., Rodgers, R. F., & Dietel, F. A. (2023). Association between engagement with appearance and eating related TikTok content and eating disorder symptoms via recommended content and appearance comparisons. *The International Journal of Eating Disorders*. Advance online publication. <https://doi.org/10.1002/eat.24117>
- Duivenvoorde, B., & Goanta, C. (2023). The regulation of digital advertising under the DSA: A critical assessment. *Computer Law & Security Review*, 51, 105870. <https://doi.org/10.1016/j.clsr.2023.105870>
- Dutt, B. (2023). Wellbeing Amid Digital Risks: Implications of Digital Risks, Threats, and Scams on Users' Wellbeing. *Media and Communication*, 11(2), 355–366. <https://doi.org/10.17645/mac.v11i2.6480>
- Ebrahim, S., & Tanner, M. (2023). The Actualization of TikTok Affordances to Challenge Female Unrealistic Standards of Beauty. In P. D. Haghighi, E. Pardede, G. Dobbie, V.

- Yogarajan, N. A. Sanjaya ER, G. Kotsis, & I. Khalil (Eds.), *Lecture Notes in Computer Science. Information Integration and Web Intelligence: 25th International Conference, IiWAS 2023, Denpasar, Bali, Indonesia, December 4-6, 2023, Proceedings* (1st ed., Vol. 14416, pp. 417–430). Cham: Springer. https://doi.org/10.1007/978-3-031-48316-5_39
- Egard, H., & Hansson, K. (2023). The digital society comes sneaking in. An emerging field and its disabling barriers. *Disability & Society*, 38(5), 761–775. <https://doi.org/10.1080/09687599.2021.1960275>
- Ekberg, M. (2007). The Parameters of the Risk Society. *Current Sociology*, 55(3), 343–366. <https://doi.org/10.1177/0011392107076080>
- El-Aawar, N. (2020). *Die Reproduktion sozialer Ungleichheit anhand der Datenökonomie: Eine kritische Analyse am Praxisbeispiel Facebook*. Unpublished Bachelor Thesis, University of Hamburg.
- El-Aawar, N. (2023). *Digitale Vergesellschaftung: Digitale Interaktionen als moderne Form der Wechselwirkung? Eine Analyse am Fallbeispiel TikTok*. Unpublished paper, University of Vienna.
- European Commission (2016). COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS: Online Platforms and the Digital Single Market Opportunities and Challenges for Europe. Retrieved from <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016DC0288>, [2023-11-14].
- European Commission (2019). Shaping Europe's digital future: How do online platforms shape our lives and businesses? - Brochure. Retrieved from <https://digital-strategy.ec.europa.eu/en/library/how-do-online-platforms-shape-our-lives-and-businesses-brochure#Facts>, [2023-11-09].
- European Commission (2020a). 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. Retrieved from <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM%3A2020%3A825%3AFIN>, [2023-11-06].
- European Commission (2020b). *Shaping Europe's digital future*. Luxembourg: Publications Office of the European Union. Retrieved from https://commission.europa.eu/system/files/2020-02/communication-shaping-europes-digital-future-feb2020_en_4.pdf.
- European Commission (2021). Final reports on the EU Observatory on the online platform economy. Retrieved from <https://digital-strategy.ec.europa.eu/en/news/final-reports-eu-observatory-online-platform-economy>, [2023-11-28].
- European Commission (2022). Shaping Europe's digital future: Tackling online disinformation. Retrieved from <https://digital-strategy.ec.europa.eu/en/policies/online-disinformation>, [2024-01-04].
- European Commission (2023a). The Digital Markets Act: ensuring fair and open digital markets. Retrieved from https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en, [2023-11-07].
- European Commission (2023b). The Digital Services Act: ensuring a safe and accountable online environment. Retrieved from <https://commission.europa.eu/strategy-and->

- policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_en, [2023-11-02].
- European Commission (2023c). Shaping Europe's digital future: The Digital Service Act package. Retrieved from <https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package>, [2023-11-02].
- European Commission (2023d). Types of EU law. Retrieved from https://commission.europa.eu/law/law-making-process/types-eu-law_en, [2023-11-01].
- European Commission, Directorate-General for Communications Networks, Content and Technology (2023). *Digital Services Act: Application of the risk management framework to Russian disinformation campaigns*. Luxembourg: Publications Office of the European Union.
- European Data Protection Board (2021). Guidelines 8/2020 on the targeting of social media users: Version 2.0. Retrieved from https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_082020_on_the_targeting_of_social_media_users_en.pdf, [2023-02-15].
- European Data Protection Board (2023a). 1.2 billion euro fine for Facebook as a result of EDPB binding decision. Retrieved from https://edpb.europa.eu/news/news/2023/12-billion-euro-fine-facebook-result-edpb-binding-decision_en, [2024-01-10].
- European Data Protection Board (2023b). EDPB Urgent Binding Decision on processing of personal data for behavioural advertising by Meta. Retrieved from https://edpb.europa.eu/news/news/2023/edpb-urgent-binding-decision-processing-personal-data-behavioural-advertising-meta_en#, [2024-01-12].
- European Data Protection Board (2023c). Facebook and Instagram decisions: “Important impact on use of personal data for behavioural advertising”. Retrieved from https://edpb.europa.eu/news/news/2023/facebook-and-instagram-decisions-important-impact-use-personal-data-behavioural_hu, [2024-01-10].
- European Parliament (2022a). Digital Services Act: agreement for a transparent and safe online environment. Retrieved from <https://www.europarl.europa.eu/news/en/press-room/20220412IPR27111/digital-services-act-agreement-for-a-transparent-and-safe-online-environment>, [2023-11-09].
- European Parliament (2022b). Digital Services: landmark rules adopted for a safer, open online environment. Retrieved from <https://www.europarl.europa.eu/news/en/press-room/20220701IPR34364/digital-services-landmark-rules-adopted-for-a-safer-open-online-environment>, [2023-11-06].
- European Union (2016). REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Retrieved from <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679>, [2023-11-14].
- European Union (2022). *REGULATION (EU) 2022/2065 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act)*. Retrieved from <https://eur-lex.europa.eu/legal->

content/EN/TXT/?toc=OJ%3AL%3A2022%3A277%3ATOC&uri=uriserv%3AOJ.L_.2022.277.01.0001.01.ENG.

- Evans, D. S. (2003). The Antitrust Economics of Two-Sided Markets. *Yale Journal on Regulation*, 20(2), 325–381. <https://doi.org/10.2139/ssrn.332022>
- Evans, D. S., & Schmalensee, R. (2016). *Matchmakers: The new economics of multisided platforms*. Boston, Massachusetts: Harvard Business Review Press. Retrieved from <https://search.ebscohost.com/login.aspx?direct=true&scope=site&db=nlebk&db=nlabk&AN=1260359>.
- Evans, D. S., Schmalensee, R., Noel, M. D., Chang, H. H., & Garcia-Swartz, D. D. (2011). *Platform Economics: Essays on Multi-Sided Businesses*. Competition Policy International.
- Faelens, L., Hoorelbeke, K., Cambier, R., van Put, J., van de Putte, E., Raedt, R. de, & Koster, E. H. (2021). The relationship between Instagram use and indicators of mental health: A systematic review. *Computers in Human Behavior Reports*, 4, 100121. <https://doi.org/10.1016/j.chbr.2021.100121>
- Fernández, M., Bellogín, A., & Cantador, I. (2021). *Analysing the Effect of Recommendation Algorithms on the Amplification of Misinformation*. arXiv. <https://doi.org/10.48550/ARXIV.2103.14748>
- Frosio, G., & Geiger, C. (2020). Taking Fundamental Rights Seriously in the Digital Services Act's Platform Liability Regime. *SSRN Electronic Journal*. Advance online publication. <https://doi.org/10.2139/ssrn.3747756>
- Fuchs, C. (2021). *Social Media: A critical introduction* (Third edition). London, Los Angeles, New Delhi, Singapore, Washington, DC, Melbourne: SAGE Publications Ltd.
- Fuchs, C., & Kurz, F. (2021). *Soziale Medien und Kritische Theorie: Eine Einführung* (2. vollständig überarbeitete Auflage). *utb-studi-e-book: Vol. 5081*. Stuttgart, Konstanz: utb GmbH; UVK. <https://doi.org/10.36198/9783838555003>
- Fung, A. C. H., & Wong, K. K. Y. (2023). Tick-tock: now is the time for regulating social media for child protection. *BMJ Paediatrics Open*, 7(1), e002093. <https://doi.org/10.1136/bmjpo-2023-002093>
- Fuster Morell, M. (2022). The gender of the platform economy. *Internet Policy Review*, 11(1). <https://doi.org/10.14763/2022.1.1620>
- Gabarron, E., Oyeyemi, S. O., & Wynn, R. (2021). Covid-19-related misinformation on social media: A systematic review. *Bulletin of the World Health Organization*, 99(6), 455-463. <https://doi.org/10.2471/BLT.20.276782>
- Galaz, V., Centeno, M. A., Callahan, P. W., Causevic, A., Patterson, T., Brass, I., . . . Levy, K. (2021). Artificial intelligence, systemic risks, and sustainability. *Technology in Society*, 67, 101741. <https://doi.org/10.1016/j.techsoc.2021.101741>
- Gawer, A., & Srnicek, N. (2021). *Online platforms: Economic and societal effects*. Brussels: European Parliament.
- Giddens, A. (1999). Risk and Responsibility. *Modern Law Review*, 62(1), 1–10. <https://doi.org/10.1111/1468-2230.00188>
- Gillespie, T. (2010). The politics of ‘platforms’. *New Media & Society*, 12(3), 347–364. <https://doi.org/10.1177/1461444809342738>
- Goldfarb, A., & Tucker, C. (2019). Digital Economics. *Journal of Economic Literature*, 57(1), 3–43. <https://doi.org/10.1257/jel.20171452>

- Grandinetti, J., & Bruinsma, J. (2023). The Affective Algorithms of Conspiracy TikTok. *Journal of Broadcasting & Electronic Media*, 67(3), 274–293. <https://doi.org/10.1080/08838151.2022.2140806>
- Gregorio, G. de, & Dunn, P. (2022). The European Risk-Based Approaches: Connecting Constitutional Dots in the Digital Age. *SSRN Electronic Journal*. Advance online publication. <https://doi.org/10.2139/ssrn.4071437>
- Grenz, T. (2023). Mediatisation, Economy, and Infrastructural Dynamics in the Digital Risk Society. In K. Kopecka-Piech & G. Bolin (Eds.), *Contemporary Challenges in Mediatisation Research* (pp. 96–110). London: Routledge. <https://doi.org/10.4324/9781003324591-9>
- Guess, A., Nyhan, B., & Reifler, J. (2018). *Selective Exposure to Misinformation: Evidence from the consumption of fake news during the 2016 U.S. presidential campaign*. Retrieved from European Research Council website: <https://about.fb.com/wp-content/uploads/2018/01/fake-news-2016.pdf>
- Haimson, O. L., Delmonaco, D., Nie, P., & Wegner, A. (2021). Disproportionate Removals and Differing Content Moderation Experiences for Conservative, Transgender, and Black Social Media Users: Marginalization and Moderation Gray Areas. *Proceedings of the ACM on Human-Computer Interaction*, 5(CSCW2), 1–35. <https://doi.org/10.1145/3479610>
- Harris, C., Johnson, A. G., Palmer, S., Yang, D., & Bruckman, A. (2023). "Honestly, I Think TikTok has a Vendetta Against Black Creators": Understanding Black Content Creator Experiences on TikTok. *Proceedings of the ACM on Human-Computer Interaction*, 7(CSCW2), 1–31. <https://doi.org/10.1145/3610169>
- Heldt, A. P. (2022). EU Digital Services Act: The White Hope of Intermediary Regulation. In T. Flew & F. R. Martin (Eds.), *Digital Platform Regulation* (pp. 69–84). Cham: Springer International Publishing.
- Hering, L., & Jungmann, R. (2022). Einzelfallanalyse. In N. Baur & J. Blasius (Eds.), *Handbuch Methoden der empirischen Sozialforschung* (pp. 677–689). Wiesbaden: Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-37985-8_42
- Hesmondhalgh, D., Valverde, R. C., Kaye, D. B. V., & Li, Z. (2023). Digital Platforms and Infrastructure in the Realm of Culture. *Media and Communication*, 11(2). <https://doi.org/10.17645/mac.v11i2.6422>
- Himelein-Wachowiak, M., Giorgi, S., Devoto, A., Rahman, M., Ungar, L., Schwartz, H. A., . . . Curtis, B. (2021). Bots and Misinformation Spread on Social Media: Implications for COVID-19. *Journal of Medical Internet Research*, 23(5). <https://doi.org/10.2196/26933>
- Huhtala, T. T. (2019). Personal data as a resource to transform the business model in a service ecosystem. Advance online publication. <https://doi.org/10.5278/OJS.JBM.V7I2.2482>
- Husovec, M., & Roche Laguna, I. (2022). Digital Services Act: A Short Primer. *SSRN Electronic Journal*. Advance online publication. <https://doi.org/10.2139/ssrn.4153796>
- Instagram. Transparency Report for Instagram. Retrieved from <https://transparency.fb.com/sr/dsa-transparency-report-oct2023-instagram/>, [2023-12-12].
- Instagram (2021). Continuing to Make Instagram Safer for the Youngest Members of Our Community. Retrieved from <https://about.instagram.com/blog/announcements/continuing-to-make-instagram-safer-for-the-youngest-members-of-our-community>, [2024-01-10].

- Instagram (2022). Data Policy. Retrieved from https://help.instagram.com/155833707900388?cms_id=155833707900388, [2023-12-21].
- Instagram (2023a). How Instagram Feed Works. Retrieved from <https://help.instagram.com/1986234648360433/>, [2023-12-26].
- Instagram (2023b). Regulation (EU) 2022/2065 Digital Services Act: Transparency Report for Instagram. Retrieved from <https://transparency.fb.com/sr/dsa-transparency-report-oct2023-instagram/>, [2024-01-09].
- Instagram (2024). Safety on Instagram. Retrieved from <https://about.instagram.com/safety/account-safety#safety-resources>.
- Jacques, E. T., Basch, C. H., Fera, J., & Jones, V. (2023). #StopAsianHate: A content analysis of TikTok videos focused on racial discrimination against Asians and Asian Americans during the COVID-19 pandemic. *Dialogues in Health*, 2, 100089. <https://doi.org/10.1016/j.dialog.2022.100089>
- Jarvis, D. (2007). Risk, Globalisation and the State: A Critical Appraisal of Ulrich Beck and the World Risk Society Thesis. *Global Society*, 21(1), 23–46. <https://doi.org/10.1080/13600820601116468>
- Jeon, D.-S. (2021). *Market power and transparency in open display advertising – a case study: Final Report, Expert Group for the Observatory on the Online Platform Economy*.
- Jin Kang, J. (2022). Adapting to Live in the Global Pandemic Era: Case Studies. In S. Adibi, A. Rajabifard, S. M. Shariful Islam, & A. Ahmadvand (Eds.), *Springer Series on Bio- and Neurosystems: Vol. 15. The Science behind the COVID Pandemic and Healthcare Technology Solutions* (1st ed., pp. 119–128). Cham: Springer International Publishing; Springer. https://doi.org/10.1007/978-3-031-10031-4_6
- Jong, A. (2022). World Risk Society and Constructing Cosmopolitan Realities: A Bourdieusian Critique of Risk Society. *Frontiers in Sociology*, 7. <https://doi.org/10.3389/fsoc.2022.797321>
- Kalbhenn, J. C. (2021). European Legislative Initiative for Very Large Communication Platforms. In J. Bayer, B. Holznagel, P. Korpisaari, & L. Woods (Eds.), *Perspectives on Platform Regulation* (pp. 47–76). Nomos Verlagsgesellschaft mbH & Co. KG.
- Karwatzki, S., Trenz, M., & Veit, D. (2022). The multidimensional nature of privacy risks: Conceptualisation, measurement and implications for digital services. *Information Systems Journal*, 32(6), 1126–1157. <https://doi.org/10.1111/isj.12386>
- Kaufman, G. G., & Scott, K. E. (2003). What is systemic risk, and do bank regulators retard or contribute to it? *Independent Review*, 7(3). Retrieved from <https://link-gale-com.uaccess.univie.ac.at/apps/doc/A96267634/ITOF?u=43wien&sid=bookmark-ITOF&xid=7ee875c8>.
- Keles, B., McCrae, N., & Grealish, A. (2020). A systematic review: the influence of social media on depression, anxiety and psychological distress in adolescents. *International Journal of Adolescence and Youth*, 25(1), 79–93. <https://doi.org/10.1080/02673843.2019.1590851>
- Kenney, M., Bearson, D., & Zysman, J. (2021). The platform economy matures: measuring pervasiveness and exploring power. *Socio-Economic Review*, 19(4), 1451–1483. <https://doi.org/10.1093/ser/mwab014>
- Keyte, R., Mullis, L., Egan, H., Hussain, M., Cook, A., & Mantzios, M. (2021). Self-Compassion and Instagram Use Is Explained by the Relation to Anxiety, Depression, and

- Stress. *Journal of Technology in Behavioral Science*, 6(2), 436–441.
<https://doi.org/10.1007/s41347-020-00186-z>
- Khan, Z., Zeng, J., Knight, G., Rajwani, T., & Pattnaik, C. (2023). Non-market strategies and disruptive innovation in the platform economy. *Journal of International Management*, 29(5), 101047. <https://doi.org/10.1016/j.intman.2023.101047>
- Knöbl, W. (2017). Bleibt alles anders: Ulrich Beck deutet die Metamorphose der Welt. *Soziopolis: Gesellschaft Beobachten*. Retrieved from <https://nbn-resolving.org/urn:nbn:de:0168-ssoar-82280-2>.
- Krotova, A., Rusche, C., & Spiekermann, M. (2019). *Die ökonomische Bewertung von Daten: Verfahren, Beispiele und Anwendungen = The economic evaluation of data : procedures, examples and applications. IW-Analysen: Vol. 129*. Köln: Institut der deutschen Wirtschaft Köln Medien GmbH.
- Kuehn, K. M., & Salter, L. A. (2020). Assessing Digital Threats to Democracy, and Workable Solutions: A Review of the Recent Literature. *International Journal of Communication*, 14(1), 2589–2610.
- Lambert, J., Barnstable, G., Minter, E., Cooper, J., & McEwan, D. (2022). Taking a One-Week Break from Social Media Improves Well-Being, Depression, and Anxiety: A Randomized Controlled Trial. *Cyberpsychology, Behavior and Social Networking*, 25(5), 287–293. <https://doi.org/10.1089/cyber.2021.0324>
- Lee, S. K., Lindsey, N. J., & Kim, K. S. (2017). The effects of news consumption via social media and news information overload on perceptions of journalistic norms and practices. *Computers in Human Behavior*, 75, 254–263. <https://doi.org/10.1016/j.chb.2017.05.007>
- Liang, Y., Aroles, J., & Brandl, B. (2022). Charting platform capitalism: Definitions, concepts and ideologies. *New Technology, Work and Employment*, 37(2), 308–327.
<https://doi.org/10.1111/ntwe.12234>
- Lohsse, S., Staudenmayer, D., & Schulze, R. (Eds.) (2017). *Trading Data in the Digital Economy: Legal Concepts and Tools: Münster Colloquia on EU Law and the Digital Economy III* (1. Auflage). Baden-Baden: Nomos Verlagsgesellschaft mbH & Co. KG.
<https://doi.org/10.5771/9783845288185>
- Loi, M. (August 2023). *Making sense of the Digital Services Act: How to define platforms' systemic risks to democracy*. Retrieved from https://algorithmwatch.org/en/wp-content/uploads/2023/08/AlgorithmWatch_Risk_Assessment-DSA.pdf.
- Longhofer, J., Floersch, J., & Hartmann, E. (2017). A Case for the Case Study: How and Why They Matter. *Clinical Social Work Journal*, 45(3), 189–200.
<https://doi.org/10.1007/s10615-017-0631-8>
- Lu, X., & Lu, Z. (2019). Fifteen Seconds of Fame: A Qualitative Study of Douyin, A Short Video Sharing Mobile Application in China. In G. Meiselwitz (Ed.), *Information Systems and Applications, incl. Internet/Web, and HCI: Vol. 11578. Social Computing and Social Media. Design, Human Behavior and Analytics: 11th International Conference, SCSM 2019, Held as Part of the 21st HCI International Conference, HCII 2019, Orlando, FL, USA, July 26-31, 2019, Proceedings, Part I* (1st ed., Vol. 11578, pp. 233–244). Cham: Springer International Publishing; Imprint: Springer. https://doi.org/10.1007/978-3-030-21902-4_17
- Luhmann, N. (2003). *Soziologie des Risikos* (Unveränd. Nachdr. der Ausg. von 1991). De-Gruyter-Studienbuch. Berlin, New York: De Gruyter.

- Lupton, D. (2016). Digital risk society. In A. Burgess, A. Alemanno, & J. Zinn (Eds.), *Routledge Handbook of Risk Studies* (pp. 301–309). Abingdon, Oxon, New York, NY: Routledge, 2016.: Routledge. <https://doi.org/10.4324/9781315776835-42>
- Lupton, D. (2020). *Data selves: More-than-human perspectives* (First published.). Cambridge, Medford, MA: Polity.
- Lupton, D. (2023). *Risk* (Third edition). *Key ideas*. Abingdon, Oxon, New York, NY: Routledge. <https://doi.org/10.4324/9781003316299>
- Madhura K., & Niyaz Panakaje (2022). Social Media as a Promotional Tool in the Fashion Industry: A Case Study on Meta Platforms Inc. Advance online publication. <https://doi.org/10.5281/ZENODO.6539694>
- Madiega, T. (2022). Adopting the digital service act. Retrieved from [https://www.europarl.europa.eu/RegData/etudes/ATAG/2022/733562/EPRS_ATA\(2022\)733562_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/ATAG/2022/733562/EPRS_ATA(2022)733562_EN.pdf), [2023-11-06].
- Mancin, P., Cerea, S., Bottesi, G., & Ghisi, M. (2023). Instagram use and negative and positive body image: the relationship with following accounts and content and filter use among female students. *Current Psychology*. Advance online publication. <https://doi.org/10.1007/s12144-023-05204-w>
- Mattern, J. (2017). *Instagram. Social media sensations*. Minneapolis, Minnesota: Checkerboard Library, an imprint of Abdo Publishing. Retrieved from <https://ebookcentral.proquest.com/lib/kxp/detail.action?docID=5262408>.
- McCashin, D., & Murphy, C. M. (2023). Using TikTok for public and youth mental health - A systematic review and content analysis. *Clinical Child Psychology and Psychiatry*, 28(1), 279–306. <https://doi.org/10.1177/13591045221106608>
- McGovern, O., Collins, R., & Dunne, S. (2022). The associations between photo-editing and body concerns among females: A systematic review. *Body Image*, 43, 504–517. <https://doi.org/10.1016/j.bodyim.2022.10.013>
- McIntyre, D. P., & Srinivasan, A. (2017). Networks, platforms, and strategy: Emerging views and next steps. *Strategic Management Journal*, 38(1), 141–160. <https://doi.org/10.1002/smj.2596>
- Medvedev, I., Gordon, T., & Wu, H. (2019). Powered by AI: Instagram’s Explore recommender system. Retrieved from <https://ai.meta.com/blog/powered-by-ai-instagram-explore-recommender-system/>, [2023-12-28].
- Meikle, G. (2016). *Social media: Communication, sharing and visibility*. New York, Abingdon, Oxon: Routledge. <https://doi.org/10.4324/9781315884172>
- Mejias, U. A., & Couldry, N. (2019). Datafication. *Internet Policy Review*, 8(4), 1–10. <https://doi.org/10.14763/2019.4.1428>
- Meta (2019). Combating Misinformation on Instagram. Retrieved from <https://about.fb.com/news/2019/12/combating-misinformation-on-instagram/>, [2024-01-09].
- Meta (2023a). Data Policy. Retrieved from <https://privacycenter.instagram.com/policy/>, [2023-12-21].
- Meta (2023b). Facebook and Instagram to Offer Subscription for No Ads in Europe. Retrieved from <https://about.fb.com/news/2023/10/facebook-and-instagram-to-offer-subscription-for-no-ads-in-europe/>, [2024-01-12].

- Meta (2023c). Privacy Center: Information from cookies and similar technologies. Retrieved from [https://privacycenter.instagram.com/policy/?annotations\[0\]=1.ex.17-CookiesCookiesAreSmall&subpage=1.subpage.3-AppBrowserAndDevice](https://privacycenter.instagram.com/policy/?annotations[0]=1.ex.17-CookiesCookiesAreSmall&subpage=1.subpage.3-AppBrowserAndDevice), [2023-12-25].
- Meta (2023d). Transparency Center: Instagram Feed AI system. Retrieved from <https://transparency.fb.com/features/explaining-ranking/ig-feed/?referrer=1>, [2023-12-28].
- Meta (2023e). Transparency Center: Our Approach to Facebook Feed Ranking. Retrieved from <https://transparency.fb.com/features/ranking-and-content/>, [2023-12-28].
- Meta (2024). Meta subscription (self-generated screenshot from Instagram). Retrieved from <https://about.fb.com/news/2023/10/facebook-and-instagram-to-offer-subscription-for-no-ads-in-europe/>.
- Möller, J. (2021). Filter bubbles and digital echo chambers. In H. Tumber & S. Waisbord (Eds.), *Routledge companions. The Routledge companion to media disinformation and populism* (2021st ed., pp. 92–100). Abingdon, New York, NY: Routledge.
- Montag, C., Yang, H., & Elhai, J. D. (2021). On the Psychology of TikTok Use: A First Glimpse From Empirical Findings. *Frontiers in Public Health*, 9, 641673. <https://doi.org/10.3389/fpubh.2021.641673>
- Montalban, M., Frigant, V., & Jullien, B. (2019). Platform economy as a new form of capitalism: a Régulationist research programme. *Cambridge Journal of Economics*, 43(4), 805–824. <https://doi.org/10.1093/cje/bez017>
- Moreton, L., & Greenfield, S. (2022). University students' views on the impact of Instagram on mental wellbeing: A qualitative study. *BMC Psychology*, 10(1), 45. <https://doi.org/10.1186/s40359-022-00743-6>
- Mouthaan, M., Frenken, K., Piscicelli, L., & Vaskelainen, T. (2023). Systemic sustainability effects of contemporary digitalization: A scoping review and research agenda. *Futures*, 149, 103142. <https://doi.org/10.1016/j.futures.2023.103142>
- Mueller, R. S., III (2019). Report on the Investigation into Russian Interference in the 2016 Presidential Election (Vol I). *1 Report on the Investigation into Russian Interference in the 2016 Presidential Election (Mar. 22, 2019).*, 1. Retrieved from <https://heinonline.org/HOL/Page?handle=hein.exprivcol/execpraaac0001&id=1&div=&collection=presidents>.
- Mustak, M., Salminen, J., Mäntymäki, M., Rahman, A., & Dwivedi, Y. K. (2023). Deepfakes: Deceptions, mitigations, and opportunities. *Journal of Business Research*, 154, 113368. <https://doi.org/10.1016/j.jbusres.2022.113368>
- Mythen, G. (2021). The Critical Theory of World Risk Society: A Retrospective Analysis. *Risk Analysis : An Official Publication of the Society for Risk Analysis*, 41(3), 533–543. <https://doi.org/10.1111/risa.13159>
- Naslund, J. A., Bondre, A., Torous, J., & Aschbrenner, K. A. (2020). Social Media and Mental Health: Benefits, Risks, and Opportunities for Research and Practice. *Journal of Technology in Behavioral Science*, 5(3), 245–257. <https://doi.org/10.1007/s41347-020-00134-x>
- Ngwenyama, O., Henriksen, H. Z., & Hardt, D. (2023). PUBLIC MANAGEMENT CHALLENGES IN THE DIGITAL RISK SOCIETY: A Critical Analysis of the Public Debate on Implementation of the Danish NemID. *European Journal of Information Systems*, 32(2), 108–126. <https://doi.org/10.1080/0960085X.2021.1907234>

- OECD (2019). *Introduction to online platforms and their role in the digital transformation*. Paris: OECD Publishing. <https://doi.org/10.1787/53e5f593-en>
- Ormrod, J. S. (2013). Beyond World Risk Society? A Critique of Ulrich Beck's World Risk Society Thesis as a Framework for Understanding Risk Associated with Human Activity in Outer Space. *Environment and Planning D: Society and Space*, 31(4), 727–744. <https://doi.org/10.1068/d16511>
- Pariser, E. (2012). *Filter bubble: Wie wir im Internet entmündigt werden* (1. Aufl.). München: Hanser. Retrieved from <http://www.hanser-elibrary.com/action/showBook?doi=10.3139/9783446431164>. <https://doi.org/10.3139/9783446431164>
- Pasquale, F. (2015). *The black box society: The secret algorithms that control money and information*. Cambridge: Harvard University Press. <https://doi.org/10.4159/harvard.9780674736061>
- Pathak, R., Spezzano, F., & Pera, M. S. (2023). Understanding the Contribution of Recommendation Algorithms on Misinformation Recommendation and Misinformation Dissemination on Social Networks. *ACM Transactions on the Web*, 17(4), 1–26. <https://doi.org/10.1145/3616088>
- Pawelec, M. (2022). Deepfakes and Democracy (Theory): How Synthetic Audio-Visual Media for Disinformation and Hate Speech Threaten Core Democratic Functions. *Digital Society*, 1(2), 19. <https://doi.org/10.1007/s44206-022-00010-6>
- Pedrouzo, S. B., & Krynski, L. (2023). Hyperconnected: Children and adolescents on social media. The TikTok phenomenon [Hyperconnected: Children and adolescents on social media. The TikTok phenomenon]. *Archivos Argentinos De Pediatría*, 121(4), e202202674. <https://doi.org/10.5546/aap.2022-02674.eng>
- Peterson-Salahuddin, C. (2022). “Pose”: Examining moments of “digital” dark sousveillance on TikTok, 1–20. <https://doi.org/10.1177/14614448221080480>
- Peticca-Harris, A., deGama, N., & Ravishankar, M. N. (2020). Postcapitalist precarious work and those in the ‘drivers’ seat: Exploring the motivations and lived experiences of Uber drivers in Canada. *Organization*, 27(1), 36–59. <https://doi.org/10.1177/1350508418757332>
- Peukert, A. (2021). Five Reasons to be Sceptical About the DSA. In H. Richter, M. Straub, & Tuchtfield, Erik (Eds.), *To Break Up or Regulate Big Tech Avenues to Constrain Private Power in the DSA/DMA Package: Avenues to constrain private power in the DSA/DMA Package* (pp. 22–27). München: (:unas).
- Plantin, J.-C., Lagoze, C., Edwards, P. N., & Sandvig, C. (2018). Infrastructure studies meet platform studies in the age of Google and Facebook. *New Media & Society*, 20(1), 293–310. <https://doi.org/10.1177/1461444816661553>
- Poell, T., Nieborg, D., & van Dijck, J. [José] (2019). Platformisation. *Internet Policy Review*, 8(4), 1–13. <https://doi.org/10.14763/2019.4.1425>
- Ponnusamy, S., Iranmanesh, M., Foroughi, B., & Hyun, S. S. (2020). Drivers and outcomes of Instagram Addiction: Psychological well-being as moderator. *Computers in Human Behavior*, 107, 106294. <https://doi.org/10.1016/j.chb.2020.106294>
- Primig, F., Szabó, H. D., & Lacasa, P. (2023). Remixing war: An analysis of the reimagination of the Russian–Ukraine war on TikTok. *Frontiers in Political Science*, 5. <https://doi.org/10.3389/fpos.2023.1085149>

- Prinzing, M. (2019). Auf dem Weg in eine Diktatur der Wahrscheinlichkeit? Fragen nach der Verantwortung beim Einsatz von Prognosesoftware. In C. Ochs, M. Friedewald, T. Hess, & J. Lamla (Eds.), *Medienkulturen im digitalen Zeitalter. Die Zukunft der Datenökonomie: Zwischen Geschäftsmodell, Kollektivgut und Verbraucherschutz* (pp. 269–284). Wiesbaden: Springer VS. https://doi.org/10.1007/978-3-658-27511-2_12
- Quinn, E. K., Fazel, S. S., & Peters, C. E. (2021). The Instagram Infodemic: Cobranding of Conspiracy Theories, Coronavirus Disease 2019 and Authority-Questioning Beliefs. *Cyberpsychology, Behavior and Social Networking*, 24(8), 573–577. <https://doi.org/10.1089/cyber.2020.0663>
- Rasborg, K. (2018). From ‘the Bads of Goods’ to ‘the Goods of Bads’: The Most Recent Developments in Ulrich Beck’s Cosmopolitan Sociology. *Theory, Culture & Society*, 35(7–8), 157–171. <https://doi.org/10.1177/0263276418810418>
- Ridder, H.-G. (2020). *Case study research: Approaches, methods, contribution to theory* (Second edition). *Sozialwissenschaftliche Forschungsmethoden: volume 12*. Augsburg, München: Rainer Hampp Verlag. Retrieved from https://www.wiso-net.de/document/EBOK,AEBO__9783957102638234.
- Riesenhuber, K. (2019). Daten als „Einnahmen“ von Nutzern urheberrechtlich geschützter Werke und Leistungen. In C. Ochs, M. Friedewald, T. Hess, & J. Lamla (Eds.), *Medienkulturen im digitalen Zeitalter. Die Zukunft der Datenökonomie: Zwischen Geschäftsmodell, Kollektivgut und Verbraucherschutz* (pp. 29–44). Wiesbaden: Springer VS. https://doi.org/10.1007/978-3-658-27511-2_3
- Rifkin, J. (2015). *The zero marginal cost society: The Internet of things, the collaborative commons, and the eclipse of capitalism*. New York: Palgrave Macmillan.
- Roberts, H., Farris, R., & Benkler, Y. (2018). *Network Propaganda*. [Erscheinungsort nicht ermittelbar]: Oxford University Press. <https://doi.org/10.1093/oso/9780190923624.001.0001>
- Rodríguez de las Heras Ballell, T. (2021). The background of the Digital Services Act: looking towards a platform economy. *ERA Forum*, 22(1), 75–86. <https://doi.org/10.1007/s12027-021-00654-w>
- Rosa, E. A. (2003). The logical structure of the social amplification of risk framework (SARF): Meta theoretical foundations and policy implications. In N. F. Pidgeon, R. E. Kasperson, & P. Slovic (Eds.), *The social amplification of risk* (pp. 47–79). Cambridge: Cambridge University Press. <https://doi.org/10.1017/CBO9780511550461.003>
- Rosa, E. A., Renn, O., & McCright, A. M. (2015). *The risk society revisited: Social theory and governance*. Philadelphia, Pa: Temple University Press.
- Ross Arguedas, A., Robertson, C. T., Fletcher, R., & Nielsen, R. K. (2022). *Echo chambers, filter bubbles, and polarisation: A literature review*. Reuters Institute for the Study of Journalism. <https://doi.org/10.60625/RISJ-ETXJ-7K60>
- Russell, A. M., Davis, R. E., Ortega, J. M., Colditz, J. B., Primack, B., & Barry, A. E. (2021). #alcohol: Portrayals of Alcohol in Top Videos on TikTok. *Journal of Studies on Alcohol and Drugs*, 82(5), 615–622. <https://doi.org/10.15288/jsad.2021.82.615>
- Saadatmand, F., Lindgren, R., & Schultze, U. (2019). Configurations of platform organizations: Implications for complementor engagement. *Research Policy*, 48(8), 103770. <https://doi.org/10.1016/j.respol.2019.03.015>

- Sadowski, J. (2019). When data is capital: Datafication, accumulation, and extraction. *Big Data & Society*, 6(1), 205395171882054. <https://doi.org/10.1177/2053951718820549>
- Sagrera, C. E., Magner, J., Temple, J., Lawrence, R., Magner, T. J., Avila-Quintero, V. J., . . . Murnane, K. S. (2022). Social media use and body image issues among adolescents in a vulnerable Louisiana community. *Frontiers in Psychiatry*, 13, 1001336. <https://doi.org/10.3389/fpsyt.2022.1001336>
- Sannon, S., Young, J., Shusas, E., & Forte, A. (2023). Disability Activism on Social Media: Sociotechnical Challenges in the Pursuit of Visibility. In A. Schmidt (Ed.), *ACM Digital Library, Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems* (pp. 1–15). New York, NY, United States: Association for Computing Machinery. <https://doi.org/10.1145/3544548.3581333>
- Sap, M., Card, D., Gabriel, S., Choi, Y., & Smith, N. A. (2019). The Risk of Racial Bias in Hate Speech Detection. In A. Korhonen, D. Traum, & L. Màrquez (Eds.), *Proceedings of the 57th Annual Meeting of the Association for Computational Linguistics* (pp. 1668–1678). Stroudsburg, PA, USA: Association for Computational Linguistics. <https://doi.org/10.18653/v1/P19-1163>
- Schaefer, S. [S.], M. Andersson, E. Bjarnason, & K. Hansson (2018). Introduction. In S. Schaefer, M. Andersson, E. Bjarnason, & K. Hansson (Eds.), *Working and Organizing in the Digital Age* (pp. 9–18). Lund: The Pufendorf Institute for Advanced Studies, Lund University.
- Schmidt, C. (2021). Der Begriff „Risiko“. In C. Schmidt (Ed.), *Risiko und Vertrauen* (pp. 9–16). Wiesbaden: Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-35385-8_2
- Schmidt, J.-H. (2018). *Social Media*. Wiesbaden: Springer Fachmedien Wiesbaden. <https://doi.org/10.1007/978-3-658-19455-0>
- Schneider, I. (2018). Bringing the state back in: Big Data-based capitalism, disruption and novel regulatory approaches in Europe. In A. R. Saetnan, I. Schneider, & N. Green (Eds.), *Routledge research in information technology and society: Vol. 21. The politics of big data: Big data, big brother?* (1st ed., pp. 129–175). London: Routledge.
- Schünemann, W. J. (2022). A threat to democracies? An overview of theoretical approaches and empirical measurements for studying the effects of disinformation. In M. D. Cavelty & A. Wenger (Eds.), *Cyber Security Politics* (pp. 32–47). London: Routledge.
- Sherlock, M., & Wagstaff, D. L. (2019). Exploring the relationship between frequency of Instagram use, exposure to idealized images, and psychological well-being in women. *Psychology of Popular Media Culture*, 8(4), 482–490. <https://doi.org/10.1037/ppm0000182>
- Sidorenko, P., Alonso López, N., & Paíno Ambrosio, A. (2023). Tiktok as a new paradigm for information in the Ukrainian War. A study from the West of the initial coverage of the conflict through this platform. *Estudios Sobre El Mensaje Periodístico*, 29(3), 737–748. <https://doi.org/10.5209/esmp.84815>
- Siegel, E. (2013). *Predictive analytics: The power to predict who will click, buy, lie or die*. Hoboken, New Jersey: John Wiley and Sons.
- Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*, 104, 333–339. <https://doi.org/10.1016/j.jbusres.2019.07.039>

- Soriano-Ayala, E., Bonillo Díaz, M., & Cala, V. C. (2023). TikTok and Child Hypersexualization: Analysis of Videos and Narratives of Minors. *American Journal of Sexuality Education*, 18(2), 210–230. <https://doi.org/10.1080/15546128.2022.2096734>
- Southwick, L., Guntuku, S. C., Klinger, E. V., Seltzer, E., McCalpin, H. J., & Merchant, R. M. (2021). Characterizing COVID-19 Content Posted to TikTok: Public Sentiment and Response During the First Phase of the COVID-19 Pandemic. *The Journal of Adolescent Health : Official Publication of the Society for Adolescent Medicine*, 69(2), 234–241. <https://doi.org/10.1016/j.jadohealth.2021.05.010>
- Spaccatini, F. (2019). Children's sexualization and appearance focus: A literature review. *Psicologia sociale*. (3), 343–368. <https://doi.org/10.1482/94939>
- Srnicek, N. (2017). The challenges of platform capitalism: Understanding the logic of a new business model. *Juncture*, 23(4), 254–257. <https://doi.org/10.1111/newe.12023>
- Srnicek, N. (2018). *Plattform-Kapitalismus*. Hamburg: Hamburger Edition HIS.
- Staab, P. (2021). *Digitaler Kapitalismus: Markt und Herrschaft in der Ökonomie der Unknappheit* (Sonderausgabe für die Bundeszentrale für politische Bildung). *Schriftenreihe / Bundeszentrale für politische Bildung: Band 10701*. Bonn: Bundeszentrale für politische Bildung.
- Statista (2024). Distribution of Instagram users worldwide as of January 2023, by age and gender. Retrieved from <https://www.statista.com/statistics/248769/age-distribution-of-worldwide-instagram-users/>, [2024-01-08].
- Strachan-Morris, D. (2012). Threat and Risk: What Is the Difference and Why Does It Matter? *Intelligence and National Security*, 27(2), 172–186. <https://doi.org/10.1080/02684527.2012.661641>
- Suarez-Lledo, V., & Alvarez-Galvez, J. (2021). Prevalence of Health Misinformation on Social Media: Systematic Review. *Journal of Medical Internet Research*, 23(1), e17187. <https://doi.org/10.2196/17187>
- Sun, H. (2023). Regulating Algorithmic Disinformation. *The Columbia Journal of Law & the Arts*, 46(4), 367–417. <https://doi.org/10.52214/jla.v46i3.11237>
- Sundberg, L. (2023). Towards the Digital Risk Society: A Review. *Human Affairs*, 0(0), 1–14. <https://doi.org/10.1515/humaff-2023-0057>
- Szakács, J., & Bognár, É. (2021). *The impact of disinformation campaigns about migrants and minority groups in the EU: Requested by the INGE committee*. Retrieved from https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/INGE/DV/2021/07-12/IDADisinformation_migrant_minorities_EN.pdf.
- Szczepański, M. (2020). *Briefing: Is data the new oil? Competition issues in the digital economy*. Retrieved from European Parliamentary Research Service website: [https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI\(2020\)646117](https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2020)646117)
- Taylor, S. H., & Brisini, K. S. (2024). Parenting the TikTok algorithm: An algorithm awareness as process approach to online risks and opportunities. *Computers in Human Behavior*, 150, 107975. <https://doi.org/10.1016/j.chb.2023.107975>
- Terren, L., & Borge, R. (2021). Echo Chambers on Social Media: A Systematic Review of the Literature. *Review of Communication Research*, 9, 99–118.
- TikTok (2020). TikTok Platform Cookies Policy. Retrieved from <https://www.tiktok.com/legal/page/global/cookie-policy/en>, [2023-12-26].

- TikTok (2022a). Get to know your audience better with TikTok Insights. Retrieved from <https://www.tiktok.com/business/en/insights>, [2024-01-15].
- TikTok (2022b). TikTok Web Cookies Policy. Retrieved from <https://www.tiktok.com/legal/page/global/tiktok-website-cookies-policy/en>, [2023-12-26].
- TikTok (2023a). Children's Privacy Policy. Retrieved from <https://www.tiktok.com/legal/page/global/childrens-privacy-policy/en>, [2024-01-08].
- TikTok (2023b). Creator Portal: How TikTok works: What is the "For You" Feed. Retrieved from <https://www.tiktok.com/creators/creator-portal/how-tiktok-works/whats-the-for-you-page-and-how-do-i-get-there/>, [2023-12-27].
- TikTok (2023c). European Union (EU) – Monthly Active Recipients Report: Information about TikTok’s Monthly Active Recipients number for the European Union. Retrieved from <https://www.tiktok.com/transparency/en/eu-mau/>.
- TikTok (2023d). Introduction to the TikTok recommendation system: (self-generated screenshot from TikTok). Retrieved from <https://www.tiktok.com/transparency/en-us/recommendation-system/>, [2023-12-28].
- TikTok (2023e). Our compliance with the Digital Service Act. Retrieved from <https://newsroom.tiktok.com/en-eu/compliance-digital-services-act-eu>, [2024-01-19].
- TikTok (2023f). Privacy Policy. Retrieved from <https://www.tiktok.com/legal/page/eea/privacy-policy/en>, [2024-01-08].
- TikTok (2023g). Privacy Policy: Effective Date: 19 November 2023. Retrieved from <https://www.tiktok.com/legal/page/eea/privacy-policy/en>, [2023-12-21].
- TikTok (2023h). Terms of Service. Retrieved from <https://www.tiktok.com/legal/page/eea/terms-of-service/en>, [2024-01-08].
- TikTok (2023i). TikTok Truths: A new series on our privacy and data security practices. Retrieved from <https://newsroom.tiktok.com/en-us/tiktok-truths-a-new-series-on-our-privacy-and-data-security-practices>, [2023-12-21].
- TikTok (2023j). TikTok's DSA Transparency Report 2023. Retrieved from <https://www.tiktok.com/transparency/en/dsa-transparency/>, [2024-01-09].
- TikTok (2023k). An update on our efforts to combat disinformation in Europe. Retrieved from <https://newsroom.tiktok.com/en-eu/an-update-on-our-efforts-to-combat-disinformation-in-europe>, [2024-01-09].
- TikTok (2024a). Combating misinformation. Retrieved from <https://www.tiktok.com/transparency/en-us/combating-misinformation/>, [2024-01-09].
- TikTok (2024b). Our approach to content moderation. Retrieved from <https://www.tiktok.com/transparency/en-us/content-moderation/>, [2024-01-09].
- TikTok (2024c). Suicide & self-harm. Retrieved from <https://www.tiktok.com/safety/en/suicide-self-harm/>, [2024-01-03].
- Trzaskowski, J. (2022). Data-driven value extraction and human well-being under EU law. *Electronic Markets*, 32(2), 447–458. <https://doi.org/10.1007/s12525-022-00528-0>
- Tucker, C. (2021). Comment on "Digital Infrastructure". In E. L. Glaeser & J. M. Poterba (Eds.), *National Bureau of Economic Research Conference Report. Economic analysis and infrastructure investment* (448-452). Chicago: University of Chicago Press.

- Turillazzi, A., Taddeo, M., Floridi, L., & Casolari, F. (2023). The digital services act: an analysis of its ethical, legal, and social implications. *Law, Innovation and Technology*, 15(1), 83–106. <https://doi.org/10.1080/17579961.2023.2184136>
- Twomey, J., Ching, D., Aylett, M. P., Quayle, M., Linehan, C., & Murphy, G. (2023). Do deepfake videos undermine our epistemic trust? A thematic analysis of tweets that discuss deepfakes in the Russian invasion of Ukraine. *PloS One*, 18(10), e0291668. <https://doi.org/10.1371/journal.pone.0291668>
- Van Dijck, J. [Jose] (2013). *The culture of connectivity: A critical history of social media*. Oxford, New York: Oxford University Press. Retrieved from <https://ebookcentral.proquest.com/lib/kxp/detail.action?docID=3055231>.
- Van Dijck, J. [José], Poell, T., & Waal, M. de (2018). *The platform society : public values in a connective world* (Vol. 1). Oxford University Press. <https://doi.org/10.1093/oso/9780190889760.001.0001>
- Vergnolle, S. (2021). Enforcement of the DSA and the DMA- What did we learn from the GDPR. In H. Richter, M. Straub, & Tuchtfield, Erik (Eds.), *To Break Up or Regulate Big Tech Avenues to Constrain Private Power in the DSA/DMA Package: Avenues to constrain private power in the DSA/DMA Package* (pp. 103–110). München: (:unas).
- Vicari, R., & Komendatova, N. (2023). Systematic meta-analysis of research on AI tools to deal with misinformation on social media during natural and anthropogenic hazards and disasters. *Humanities and Social Sciences Communications*, 10(1). <https://doi.org/10.1057/s41599-023-01838-0>
- Vinichenko, M. V., Nikiporets-Takigawa, G. Y., Chulanova, O. L., & Ljapunova, N. V. (2021). Threats and risks from the digitalization of society and artificial intelligence: Views of generation Z students. *International Journal of ADVANCED and APPLIED SCIENCES*, 8(10), 108–115. <https://doi.org/10.21833/ijaas.2021.10.012>
- Vorotilov, V., & Shugaepov, I. (2023). Scaling the Instagram Explore recommendations system. Retrieved from <https://engineering.fb.com/2023/08/09/ml-applications/scaling-instagram-explore-recommendations-system/>, [2023-12-28].
- Wahid, S. (2023). How to Get Away With Discrimination: The Use of Algorithms to Discriminate in the Internet Entertainment Industry. *The American University Journal of Gender, Social Policy & the Law*, 31(1), 107–139.
- Wang, W., & Wu, J. (2021). Research Perspectives on TikTok & Its Legacy Apps| Short Video Platforms and Local Community Building in China. *International Journal of Communication*, 15(0), 23. Retrieved from <https://ijoc.org/index.php/ijoc/article/view/14545>.
- Weimann, G., & Masri, N. (2021). TikTok's Spiral of Antisemitism. *Journalism and Media*, 2(4), 697–708. <https://doi.org/10.3390/journalmedia2040041>
- Wessels, N., Laubach, A., & Buxmann, P. (2019). Personenbezogene Daten in der digitalen Ökonomie – Eine wirtschaftliche und juristische Betrachtung. In C. Ochs, M. Friedewald, T. Hess, & J. Lamla (Eds.), *Medienkulturen im digitalen Zeitalter. Die Zukunft der Datenökonomie: Zwischen Geschäftsmodell, Kollektivgut und Verbraucherschutz* (pp. 11–27). Wiesbaden: Springer VS. https://doi.org/10.1007/978-3-658-27511-2_2
- Widner, J., Woolcock, M. [Micheal], & Ortega Nieto, D. (2022). Using Case Studies to Enhance the Quality of Explanation and Implementation. In J. Widner, M. Woolcock, & D.

- Ortega Nieto (Eds.), *Social Sciences. The case for case studies: Methods and applications in international development* (pp. 1–26). Cambridge: Cambridge University Press.
- World Health Organization (2024). Infodemic. Retrieved from https://www.who.int/health-topics/infodemic#tab=tab_1, [2024-01-04].
- Worschech, S., Eigmüller, M., & Büttner, S. M. (2022). Sociology of Europeanization: An Introduction. In S. M. Büttner, M. Eigmüller, & S. Worschech (Eds.), *Sozialwissenschaftliche Einführungen: Vol. 3. Sociology of Europeanization* (pp. 3–25). München, Wien: De Gruyter Oldenbourg.
- Xue, C., Tian, W., & Zhao, X. (2020). The Literature Review of Platform Economy. *Scientific Programming*, 2020, 1–7. <https://doi.org/10.1155/2020/8877128>
- Yin, R. K. (2018). *Case study research and applications : design and methods*. SAGE.
- Zambetti, M., Adrodegari, F., Pezzotta, G., Pinto, R., Rapaccini, M., & Barbieri, C. (2023). From data to value: conceptualising data-driven product service system. *Production Planning & Control*, 34(2), 207–223. <https://doi.org/10.1080/09537287.2021.1903113>
- Zeng, J., Abidin, C., & Schäfer, M. S. (2021). *Research perspectives on TikTok and its legacy apps: introduction*. University of Southern California. <https://doi.org/10.5167/uzh-205427>
- Zuboff, S. (2019). *The age of surveillance capitalism: The fight for the future at the new frontier of power*. London: Profile Books.