Hochschule Macromedia für angewandte Wissenschaften,
University of Applied Sciences

MASTERARBEIT

zur Erlangung des akademischen Grades
Master of Arts

Der neue Datenschutz
Die Auswirkungen der DSGVO auf die Privatsphäre der Nutzer und das Online Marketing

im Studiengang **Open Media Master**

Medien- und Kommunikationsmanagement

Digital Entrepreneurship

Erstprüfer:
Prof. Dr. Dominik Pietzcker

Zweiter Erstprüfer:
Prof. Dr. Astrid Friese

Vorgelegt von:
Florian Kugler
H-29648
Open Media Master
Medien- und Kommunikationsmanagement

Hamburg, im Juli, 2018

Zusammenfassung

Daten bestimmen unseren Alltag, beschleunigen den technologischen Fortschritt und lassen unsere Privatsphäre zur Illusion werden. Daten sind der Grund warum Unternehmen wie Facebook und Google heute so erfolgreich sind und immer wertvoller werden und Bürger durch politische Kampagnen instrumentalisiert werden können. Daten werden als das Erdöl des 21. Jahrhunderts bezeichnet. Der Autor dieser Arbeit hat es sich zum Ziel gesetzt, einen Weg zu skizzieren, wie Staaten, Unternehmen und Nutzer gemeinsam einen Prozess anstoßen können, der die Endkonsumenten besser schütz, ohne den technologischen und wirtschaftlichen Fortschritt zu beschneiden. Um eine Grundlage für die Entwicklung eigener Handlungsempfehlungen zu legen, wird die Privatsphäre der Nutzer im Kontext digitaler Datenverarbeitung und die in der Forschung akzeptierten Phänomene des Privacy Calculus und Privacy Paradoxons untersucht. Unter Berücksichtigung der aktuellen Gesetzeslage in Deutschland und Europa, wird der für den Datenschutz relevante Begriff der personenbezogenen Daten untersucht und Auffälligkeiten im Nutzerverhalten bei digitalen Diensten identifiziert. Auf dieser theoretischen Grundlage wurde die Kernhypothese dieser Arbeit geprüft, dass die neue Datenschutzgrundverordnung (DSGVO) der Europäischen Union Auswirkungen auf die Privatsphäre der Nutzer, die User Experience und Online Marketing-Prozesse haben wird. Um die für die Forschungsfrage relevanten Inhalte der DSGVO hervorzuheben, wurde ihr Anwendungsbereich auf Online Marketing Prozesse und Betroffenenrechte beleuchtet und zentrale Neuerungen präsentiert. Hierdurch kann das Zwischenfazit gezogen werden, dass Unternehmen und Nutzer sich mit Veränderungen konfrontiert sehen müssen. Die Kernhypothese dieser Arbeit wird anhand eines binären Forschungsdesigns überprüft, welches sich zum einen aus leitfadengestützten Interviews mit Experten aus den Bereichen Online Marketing und Datenschutz und zum anderen aus einer Gruppendiskussion mit Nutzern digitaler Dienste zusammensetzt.

Diese Untersuchung bestätigt, dass die DSGVO konkrete Auswirkungen auf Unternehmensprozesse, die Online Marketing Landschaft und auf das Nutzerverhalten hat. Trotz eines großen Mehraufwandes für Unternehmen, wird die DSGVO als positiver Schritt zu mehr Datensicherheit, gestärkter Datensouveränität und informationeller Selbstbestimmung der Nutzer wahrgenommen. Datenschutzrechtlichen Gefährdungen der Nutzer kann jedoch nicht gänzlich vorgebeugt werden, da sich der digitale Mensch als paradox handelnder Nutzer charakterisieren lässt. Datenschutz muss von Unternehmen im Sinne des Nutzers umgesetzt werden muss. Es wird neben Gesetzen, der Entwicklung innovativer Systeme zum Datenschutz und einer Bereitschaft und Kompetenz des Nutzers bedürfen, um personenbezogene Daten zukünftig besser zu schützen.

Abstract

Data determines our everyday lives, accelerates technological progress and turns our privacy into an illusion. Data is the driving force that makes the most valuable companies of today so successful and enables the instrumentalisation of citizens through political campaigns. Data is referred to as the petroleum of the 21st century. The author of this work has set up the goal to ascertain a way for states, businesses and users to work together in initiating a process that improves consumer protection and does not restrict technological and economic progress. In order to provide a basis for the development of own recommendations for action, the privacy of the users in the context of digital data processing and the scientifically accepted phenomena of the Privacy Calculus and Privacy Paradox are examined. Considering the current legal situation in Germany and Europe, the concept of personal data relevant to data protection is examined in order to describe the common user behaviour in digital services. Based on this theoretical foundation, the core hypothesis of this paper is examined that the new General Data Protection Regulation (GDPR) of the European Union will have an impact on user privacy, user experience and online marketing processes. In order to emphasize the contents of the GDPR relevant to the research question, its application on online marketing and data subjects is examined and central changes to those fields are presented. This provides an interim conclusion that companies and users will be confronted with changes. The core hypothesis of this work will be examined by means of a binary research design, which consists of guide interviews with experts from the fields of online marketing and data protection as well as a group discussion with users of digital services.

This investigation validates that the GDPR has tangible effects on business processes, the online marketing landscape and user behaviour. Despite a great deal of extra work for companies, the GDPR is perceived as a positive step towards more data security, strengthened data sovereignty and informational self-determination of users. However, privacy-related threats to users cannot be completely prevented because the digital human being can be characterized as a paradoxically acting user and data protection must also be implemented by companies in the user's sense. In addition to laws, innovative systems for data protection and the willingness and competence of the user will be necessary to better protect personal data.

Schlüsselbegriffe

Datenschutz

Informationelle Selbstbestimmung

Privatsphäre im Netz

Online Marketing

Nutzerverhalten

Key Words

Data Protection

Informational self-determination

ePrivacy

Online Marketing

User Behaviour

Inhaltsverzeichnis

Abbildungsverzeichnis

Abkürzungsverzeichnis

Abs.	Absatz
AdTech	Advertising Technology
AGB	Allgemeine Geschäftsbedingungen
AI	Artificial Intelligence
APCO	Antecedents-Privacy-Concerns-Outcome
Art.	Artikel
BDSG	Bundesdatenschutzgesetz
Bspw.	Beispielsweise
BVerfG	Bundesverfassungsgericht
Bzw.	Beziehungsweise
CDR	Corporate Digital Responsibility
DMP	Data Management Platform
DNA	Deoxyribonucleic Acid
DNT	Do not track
DSP	Data Supply Platform
DSGVO	Datenschutzgrundverordnung
DSRL	Datenschutzrichtlinie
EG	Europäische Gemeinschaft
ePVO	ePrivacy Verordnung
EU	Europäische Union
GDPR	General Data Protection Regulation
GG	Grundgesetz
GPS	Global Positioning System
ID	Identity Document
NSA	National Security Agency
PR	Public Relations
OECD	Organisation für wirtschaftliche Zusammenarbeit und Entwicklung
TMG	Telemediengesetz
TOMs	Technische und organisatorische Maßnahmen
u.a.	unter anderem
US	United States
USA	United States of America
UX	User Experience

1 Einleitung

Rund 81% der Deutschen nutzen das Internet regelmäßig, bei den 14-29 Jährigen sind es 99% (Initiative D21, 2018, S. 10). Weltweit sind rund 2,2 Milliarden Menschen monatlich bei Facebook aktiv, fast 1,5 Milliarden hiervon täglich (Facebook, 2018, S. 2 f.). Deutlich mehr als ein Viertel der Menschheit hinterlässt also personenbezogene Datenspuren bei nur einem Unternehmen. Stimmen werden immer lauter, dass die große Euphorie des technisch digitalen Fortschritts ein Ende gefunden hat (Werner & Buttlar, 2018), zu real ist die Gefahr geworden von Unternehmen abgehört und analysiert zu werden (Galloway, 2017, S. 2). Die jüngsten Enthüllungen über das große Datenleck des sozialen Netzwerks Facebook im Zuge des US-Wahlkampfs 2016 stimmen bedenklich. Die auf Nutzerdaten basierte Aussteuerung politisch motivierter und finanzierter Werbekampagnen durch das Datenanalyse-Unternehmen Cambridge Analytica zeigt, von welch großer Relevanz das Thema Datenschutz aktuell ist. Datenschutzrechtsverletzungen wie diese bestärken den Ruf nach neuen Gesetzesgrundlagen, welche die Rechte der Nutzer stärken, ihre Privatsphäre schützen und Unternehmen zu einem verantwortungsbewussten und transparenten Umgang mit Nutzerdaten verpflichten.

Die am 25. Mai 2018 in Kraft getretene Datenschutzgrundverordnung der Europäischen Union birgt verschärfte Regeln für die Datenverarbeitung durch Unternehmen, welche weitreichende Auswirkungen auf den europäischen Markt, das Nutzererlebnis und den Erfolg von Geschäftsmodellen im eBusiness haben könnten. Eine genaue Prognose über die Folgen der DSGVO abzugeben, ist ein schwieriges Unterfangen. Es wird sich erst zeigen müssen, wie Unternehmen ihre Arbeitsprozesse in Bezug auf Datenverarbeitung umstellen, in welchem Maße die Nutzer ihre Einwilligung zur Datenverarbeitung erteilen und welche Präzedenzfälle sich durch die neuen Pflichten ergeben werden. Die jüngste Vergangenheit hat gezeigt, dass selbst Skandale in Bezug auf Datenschutzrechtsverletzungen, wie die NSA-Affäre nicht dazu führen, dass die Nutzer ihren Konsum einschränken und ihr digitales Nutzungsverhalten überdenken. Durch die DSGVO soll nun die Selbstbestimmung der Nutzer gestärkt werden. Gesetze können jedoch schwer dafür sorgen, dass die Nutzer ihre Privatsphäre nicht weiterhin gegen eine scheinbar kostenlose Nutzung von Online-Diensten eintauschen. Vielmehr drängen immer mehr Geschäftsmodelle in den Markt, die auf Vernetzung, Big Data, künstlicher Intelligenz oder Ortungssystemen basieren. Viele dieser Produkte und Dienstleistungen erleichtern den Alltag, schaffen einen wirtschaftlichen Mehrwert und stehen sinnbildlich für die Digitalisierung der heutigen Industriegesellschaften. Dienste wie Google Maps, mobile Applikationen, Smartphones und Smart Home Devices sind deswegen so nützlich, weil sie auf Basis von Nutzer- und Bewegungsdaten entwickelt und verbessert wurden. Es

scheint kaum noch Lebensbereiche zu geben, die nicht im Einflussbereich digitaler Daten liegen (Reigeluth, 2015, S. 21).

Dem gegenüber steht die Gefahr der Aufgabe der informationellen Privatsphäre der Nutzer, durch eine zunehmende Integration von datenverarbeitenden Informationssystemen in den Alltag (Buck, Stadler, Suckau, & Eymann, 2016, S. 57). Personenbezogene Daten sind die Währung, die der Nutzer für die „kostenlose“ Nutzung eines sozialen Netzwerks wie Facebook oder eines kostenlosen E-Mail-Accounts von Google bezahlen. Daten die einen enormen Wert für Unternehmen haben und ein sehr präzises Porträt eines einzelnen Menschen zeichnen können. Aufgrund des hohen Verarbeitungswertes werden Daten oftmals als das Erdöl des 21. Jahrhunderts bezeichnet (Dold & Krieger, 2016, S. 1). Daten wird also ein hoher Wert und eine universelle Nutzbarkeit zugeschrieben, die ökonomische Forschung steht bei der Bewertung von personenbezogenen Daten jedoch noch mehr oder weniger am Anfang (Jentzsch, 2014, S. 793). Der tatsächliche Wert von persönlichen Daten, also die Nutzbarmachung, ist meist nicht transparent für die Nutzer. Facebook und Google nutzen all die Spuren, die ihre Nutzer durch ihr Nutzungsverhalten, ihre „Likes“, ihre Suchanfragen und durch Keywords in privaten Nachrichten hinterlassen, um ihren Werbekunden möglichst präzise Zielgruppen anbieten zu können.

Aufgrund intransparenter Information durch die Websitebetreiber wissen die Nutzer oftmals nicht, welche Daten sie eigentlich preisgeben, an wen diese weitergegeben werden und welchen Nutzen sie davon haben. Die neue Datenschutzgrundverordnung der Europäischen Union soll genau diese Diskrepanz beseitigen. Das unkontrollierte und gänzlich intransparente Datensammeln der digitalen Unternehmen soll ein Ende haben. Anstelle von versteckten Tracking-Algorithmen soll eine transparente Informationspflicht und eine deutliche Stärkung der Rechte der betroffenen Person treten. Wichtig wird hierbei jedoch sein, dass man dem digitalen Fortschritt nicht zu sehr beschneidet und den europäischen Unternehmen nicht die Handlungsfähigkeit nimmt, um im internationalen Wettbewerb konkurrenzfähig zu bleiben. In dieser Arbeit soll anhand der neuen Datenschutzgrundverordnung der Europäischen Union und fachspezifischer Literatur in den Feldern des Datenschutzes und Online-Marketings eine Prognose erarbeitet werden, wie sich die Verarbeitung von Daten, die darauf basierende Wertschöpfung sowie ein selbstbestimmterer Nutzer in Zukunft durch verschärften Datenschutz in Einklang bringen lassen.

2 Vorgehensweise, Relevanz und Zielsetzung

Bevor auf die Zielsetzung und die behandelte Thematik dieser Arbeit genauer eingegangen wird, ist zu erwähnen, dass aus stilistischen Gründen hauptsächlich auf das generische Maskulinum zurückgegriffen wird. Aufgrund der hohen Aktualität der Thematik, des direkten Zusammenhangs mit der am 25. Mai, 2018 in Kraft getretenen DSGVO und besonders durch die sich kontinuierlich weiterentwickelnde Technologie im Bereich digitaler Dienste, wird ein Fokus auf die Aktualität der gesichteten Literatur und auf eine qualitative Erhebung von Expertenstimmen aus der Online Marketing Branche und des Datenschutzrechts gelegt. Da es nicht Ziel dieser Arbeit ist, eine juristische Übersetzung der DSGVO abzubilden und als Vorlage für unternehmerische Adaption der neuen Datenschutzregeln zu dienen, werden neben den Gesetzestexten, vor allem auch Literatur verwendet, die das Thema Datenschutz auf einer ethischen Ebene behandelt und die Rolle des Nutzers in den Vordergrund hebt. Dennoch sollen marktrelevante Praktiken wie das Online Marketing in einen datenschutzbasierten Kontext gehoben und diskutiert werden, um die wirtschaftliche Bedeutung von Daten nicht außer Acht zu lassen, wenn eine Beurteilung des heutigen Datenschutzes vorgenommen wird. Hierbei soll vor allem die Privatsphäre der Nutzer und ihr Grad an informationeller Selbstbestimmung unter dem Einfluss von Online-Werbung und im Kontext ihrer Datenpreisgabe untersucht werden. Die für diese Untersuchung relevanten Erkenntnisse aus der Privatsphärenforschung werden ebenso präsentiert, wie die für diese Untersuchung relevanten Passagen der DSGVO. Ziel dieser Arbeit ist es letztendlich zu bewerten, ob Gesetzestexte wie die DSGVO in der Lage sind, die informationelle Selbstbestimmung der Nutzer zu gewährleisten, den Nutzer ausreichend zu schützen und markteffizient umsetzbar sind. Sollte sich diese Wirkung gar nicht oder nicht ausreichend feststellen lassen, sollen alternative Verfahren hergeleitet werden und diskutiert werden, die dieser Zielsetzung gerecht werden könnten. Letztendlich soll diese Arbeit auch dazu dienen eine Zukunftsprognose abzugeben, wie sich der Umgang mit Daten in der nahen Zukunft zum einen entwickeln wird und zum anderen entwickeln muss.

3 Daten und Privatsphäre

Bevor eine Einschätzung der Folgen der DSGVO und eines verstärkten Datenschutzrechts vorgenommen wird, soll ein spezieller Fokus auf Nutzerdaten, Datenströme, den Nutzen von Daten und die Privatsphäre der Nutzer gelegt werden. Im folgenden Kapitel sollen diese Themenbereiche anhand aktueller und fachspezifischer Literatur untersucht und im Hinblick auf Online Marketing Prozesse und den Nutzen von digitalen Produkten und Dienstleistungen erläutert werden, um eine fundierte Grundlage für die folgenden empirischen Methoden sowie einer Beurteilung der DSGVO zu geben. Neben Definitionsansätzen für Schlüsselbegriffe der Datenschutzthematik, sollen ebenfalls Phänomene wie das Privacy Paradoxon, Vor- und Nachteile von datengetriebenen Prozessen und die Beschaffenheit von einzigartigen Nutzerprofilen beschrieben werden. Zunächst werden Daten im digitalen Kontext betrachtet, um den relevanten Grundrahmen für diese Arbeit zu skizzieren.

Grundlegend können Daten als Rohmaterial verstanden werden, mit dem unser Gehirn umgeht und die es verarbeitet. Seit der Entwicklung von Computern werden Daten als maschinell gespeicherte Informationen verstanden, die in letzter Zeit am meisten mit ihrer Übermittlung und Verarbeitung in Verdingung gebracht werden und die in Form von Metadaten kategorisiert und indiziert werden (Reigeluth, 2015, S. 23 zit. n. Faure 2013). Ein speziell in den letzten Jahren allgegenwärtiges Thema im Datenkontext und für diese Arbeit zentrales Feld ist „Big Data“. Big Data kann als große Datenmenge begriffen werden, die nach herkömmlichen Mitteln durch ihre Heterogenität nicht auswertbar ist und deswegen über Rückgriff auf technologische Hilfsmittel ausgewertet und nutzbar gemacht wird (Hornung & Herfurth, 2018, S. 150). „Das hinter Big Data liegende Versprechen besteht darin, dass die massenhafte Aggregation von Daten, ihre gewaltigen Dimensionen und ihre induktive Korrelation uns näher als jemals zuvor an die Wirklichkeit heranführen (Reigeluth, 2015, S. 21).“

Durch die Nutzung digitaler Produkte und Dienste hinterlassen Konsumenten täglich Datenspuren, die durch Unternehmen in großen Datensätzen zusammengeführt werden. Ein weiteres Charakteristikum von Big Data ist die Verarbeitung von Datenströmen verschiedenster Formate in Echtzeit (Horstmann, 2018, S. 151). Unternehmen können mit großen Datensätzen starke Kontrolle ausüben (Bruns, Dang-Xuan, Neuberger, & Stieglitz, 2014, S. 89 f.), in etwa Geschmäcker steuern oder wie am Beispiel Cambridge Analytica zu sehen, Menschen für politische Zwecke mobilisieren. Bei der Preisgabe von Daten kann man von einer Transaktion sprechen, die sich in einem sozialen Netzwerk zunächst als reine Informationstransaktion und bei einem Online-Kauf als Informations- und Gütertransaktion definieren lässt (Jentzsch, 2014, S. 794). So bezahlt man in einem

sozialen Netzwerk mit seinen Profildaten für die Nutzung, während bei einem Online-Kauf die Daten weniger offensichtlich preisgegeben werden. In beiden Fällen kann von personenbezogenen Daten gesprochen werden, da Nutzerprofile in sozialen Netzwerken und auf eCommerce Websites in der Regel keine Pseudonyme, sondern der tatsächliche Name, E-Mail-Adressen und Kontaktdaten hinterlegt werden. Lassen Daten einen Personenbezug zu, so greift in der Regel der Datenschutz.

3.1 Personenbezogene Daten

Grundlegend für den Untersuchungsschwerpunkt dieser Arbeit, ist der Begriff der personenbezogenen Daten, für den ein Definitionsansatz in der DSGVO gegeben wird. Personenbezogene Daten sind laut Begriffsbestimmung der DSGVO, „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person […] beziehen (Art. 4 Abs. 1 DSGVO).“ Der Berliner Rechtsanwalt und Datenschutzexperte Professor Niko Härting (2016, S. 17) bewertet die Begriffsbestimmung durch die DSGVO als nach wie vor unscharf und verweist darauf, dass auch andere zentrale Begriffe wie Anonymität und Pseudonymität einigen Auslegungsspielraum bieten. Der Personenbezug ist ein entscheidendes Kriterium und Grundlage für die Anwendung des Datenschutzrechts, so ist die Datenverarbeitung von personenbezogenen Daten nach dem Verbotsprinzip nach § 4 Abs. 1 BDSG grundsätzlich nicht erlaubt (Härting, 2016, S. 17). Personenbezug besteht immer dann, wenn die Bestimmung einer Person möglich ist, also verschiedene Merkmale erfasst werden, die zwar allgemein sind, wie das Geschlecht, jedoch in Kombination mit weiteren allgemeinen Charakteristika, wie Beruf oder Postleitzahl, auf eine bestimmte Person schließen lassen. Laut Datenschutzbehörde weisen zum Beispiel auch IP-Adressen, Cookies, Online Identifier, Pseudonyme oder E-Mail-Adressen einen Personenbezug auf und dürfen somit grundsätzlich nicht verarbeitet werden (Härting, 2016, S. 72). Eine Verarbeitung war somit bereits vor Inkrafttreten der DSGVO zustimmungsbedürftig und wurde beispielsweise durch Cookie-Banner rechtlich gelöst. Wenn Daten ohne Zustimmung des Nutzers erhoben wurden, konnte bisher häufig mit einer Relativierung des Personenbezugs argumentiert werden, wenn ein absoluter Personenbezug nicht klar vorlag. Mit der DSGVO wird am absoluten Verständnis des Personenbezugs festgehalten, eine Relativierung wird jedoch deutlich schwieriger zu vertreten sein (Härting, 2016, S. 73 ff.). Dies kann als Indiz dafür gedeutet werden, dass mit Inkrafttreten der DSGVO ein Opt-In auf jeder Website, die beispielsweise Cookies mit IP-Adressen verbindet, von Nöten sein wird.

Gängige Mittel des Persönlichkeitsschutzes sind Anonymisierung sowie Pseudonymisierung, die genutzt werden, um einen klaren Personenbezug zu vermeiden. Beide Begrifflichkeiten sind Justierungen durch die DSGVO ausgesetzt. Laut § 3 Abs. 6 BDSG bedeutet Anonymisieren, „das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßigen großen Aufwand, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren Person zugeordnet werden können (Härting, 2016, S. 75).“ Hierbei kann zwischen absoluter und faktischer Anonymität unterschieden werden. Während die absolute Anonymität die Bestimmung einer Person unmöglich macht, ist die Bestimmung bei faktischer Anonymität nicht ausgeschlossen und nur über einen enormen Mehraufwand möglich (ebd.). Bei der heutigen Datenlage, den vielen Spuren, die speziell im Internet hinterlassen werden, ist eine absolute Anonymität kaum vorstellbar. Da bei faktischer Anonymität ein Personenbezug hergestellt werden kann, kann das Datenschutzrecht uneingeschränkt auf diese angewendet werden. Diese Feststellung wird auch durch die DSGVO bestätigt, eine Unterscheidung zwischen faktischer und absoluter Anonymität wird jedoch aufgegeben, somit sind gänzlich anonyme Daten nicht vom Datenschutzrecht betroffen, jedoch greift die DSGVO, sobald ein Personenbezug in irgendeiner Weise hergestellt werden kann (Härting, 2016, S. 76). Während einer Anonymisierung also keine große Bedeutung mehr beigemessen wird, ist die Pseudonymisierung, also das Ersetzen eines Namens durch ein Pseudonym, laut DSGVO ein geeignetes Mittel des Persönlichkeitsschutzes, da so die Risiken für die betroffene Person gesenkt werden können und die Einhaltung der Datenschutzpflichten für den Auftragsverarbeiter unterstützt werden (Härting, 2016, S. 77).

Personenbezogene Daten sind also trotz Unschärfe der zentrale Faktor für die Anwendung der DSGVO, während die Praktiken zum Persönlichkeitsschutz wie Anonymisierung und Pseudonymisierung immer mehr an Bedeutung verlieren. Diese Annahme wird besonders dadurch verstärkt, dass die hochfrequentierten Netzwerke wie Google oder Facebook sich dadurch definieren lassen, dass Nutzer in der Regel nicht pseudonymisierte Accounts, sondern ihren tatsächlichen Namen verwenden. Ebenfalls ist eine Preisgabe von persönlichen Informationen unumgänglich, wenn man Kunde bei jeglichen eCommerce-Unternehmen ist. Dieser offene Umgang mit personenbezogenen Daten wird nochmals verstärkt durch die Login-Möglichkeiten, die Facebook und Google ihren Nutzern auf etlichen Websites und Applikationen bieten, die zwar stark zu einem flüssigen und einheitlichen Nutzererlebnis beitragen, jedoch auch dann einen Personenbezug möglich machen, wenn dieser nicht nötig wäre. Personenbezogene Daten können heute als Wirtschaftsgut betrachtet werden, welches die Grundlage interner und externer Geschäftsprozesse darstellt (Voigt & Bussche, 2018, S. V). Ein klare Regelung für eine

Verwendung von Daten gestaltet sich auch deswegen so schwierig, da Daten als Informationen Charakteristika eines öffentlichen Gutes aufweisen und Dritte nur schwer von der Verwendung ausgeschlossen werden können, sobald diese einmal publik geworden sind (Dold & Krieger, 2016, S. 2). Im Folgenden wird das Spannungsverhältnis dieses Wirtschaftsgut mit individueller Privatsphäre, Nutzerverhalten und informationeller Selbstbestimmung tiefergehend betrachtet und mit Verschärfungen im Datenschutz und der neuen Datenschutzgrundverordnung der Europäischen Union in Verbindung gebracht.

3.2 Privatsphäre im Netz

> "If you want to keep a secret, you must also hide it from yourself."
> - George Orwell, 1984

Das Recht auf Privatsphäre ist ein Menschenrecht, das in Deutschland nach Artikel 10 und Artikel 13 im Grundgesetz verankert ist (Epping, 2017, S. 332). Mit den Einführungen geheimer Wahlen ab 1856 wurde Privatsphäre erstmals ein Politikum. Seit dem Ende des 19. Jahrhunderts ist das Recht auf Privatsphäre gesetzlich verankert. Heute zu Zeiten von Google, Facebook und Big Data, wird sie zur Illusion (Weigend, 2017, S. 74). Ursprungsdefinitorisch bedeutet Privatsphäre die legitime Verweigerung von Zugriff auf das Persönliche, oder persönliche Informationen (Bellman, 1981, S. 5). Ebenfalls kann Privatsphäre als Anspruch eines Nutzers gesehen werden, eigenständig bestimmen zu können welche Informationen für andere zugänglich sind (Buck, Stadler, Suckau, & Eymann, 2016, S. 58 zit. n. Westin 1967). Der Begriff an sich ist sehr vielschichtig und relevant für etliche Lebensbereiche und Beziehungsverhältnisse. In dieser Arbeit, soll der Begriff Privatsphäre im Kontext von Nutzerdaten und Datenspeicherung definiert werden. Hierfür lässt sich eine erste Unterteilung vornehmen, die zwischen informationeller und physischer Privatsphäre unterscheidet. Während sich die physische Privatsphäre auf die Umwelt von und den direkten Zugang zu Personen bezieht, beschreibt die informationelle Privatsphäre den Zugang zu Informationen über Personen (Eling, 2017, S. 9 zit. n. Smith et al. 2011). Nachdem zu Beginn dieses Kapitels Daten als Informationen definiert wurden, kann die informationelle Privatsphäre jetzt in einen datenbezogenen Kontext gehoben werden. Die meisten Nutzer verwenden auf Plattformen wie Facebook, Google oder Amazon anstelle von pseudonymisierten Benutzernamen, ihren echten Namen und geben überdies Kontaktdaten, Kontoinformationen und persönliche Vorlieben an. Personenbezogene Daten, welche sie bewusst oder unbewusst an die Unternehmen und anderen Werbekunden weitergeben, um „kostenlose" Produkte

nutzen zu können, damit die bestellte Ware auch an die eigene Adresse geliefert wird und der Content, den sie konsumieren, an ihre Interessen angepasst ist.

Bei der Preisgabe persönlicher Informationen wird in der Theorie eine Abwägung vorgenommen, die die Vorteile einer Nutzung, den Kosten und Risiken gegenüberstellt, die diese mit sich bringt. Hier wird die Privatsphäre also in gewisser Weise als Wert begriffen, den man gegen wahrgenommene Vorteile eintauscht (Gerber, Volkamer, & Gerber, 2017, S. 141 zit. n. Bennet 1995). Dieses Verfahren wird in der Privatsphärenforschung als „Privacy Calculus“ oder Privatsphärekalkül bezeichnet. Der Begriff Kalkül setzt voraus, dass Individuen sich über die Konsequenzen ihrer Handlungen bewusst sind, ökonomisch betrachtet also eine Kosten-Nutzen-Abwägung vornehmen. Bequemlichkeit, eine flüssige User Experience und Personalisierung aufgrund Profilierung sind einige der Gründe, die auf die Privatsphärenbedenken einwirken. Neben der kalkulierten Abwägung ist Vertrauen ebenfalls ein Einflussfaktor, der auch in dem „Antecedents-Privacy-Concerns-Outcome“-Modell (APCO-Modell) nach Smith einbezogen wird (Eling, 2017, S. 12 zit. n. Smith et al. 2011). Neben der geschilderten Abwägung und dem Vertrauen gegenüber dem Unternehmen bezieht das Modell ebenfalls staatliche Regulierungen (Abb. 1) ein und ist aus diesem Grund sehr aussagekräftig im Kontext von Datenschutz und der DSGVO.

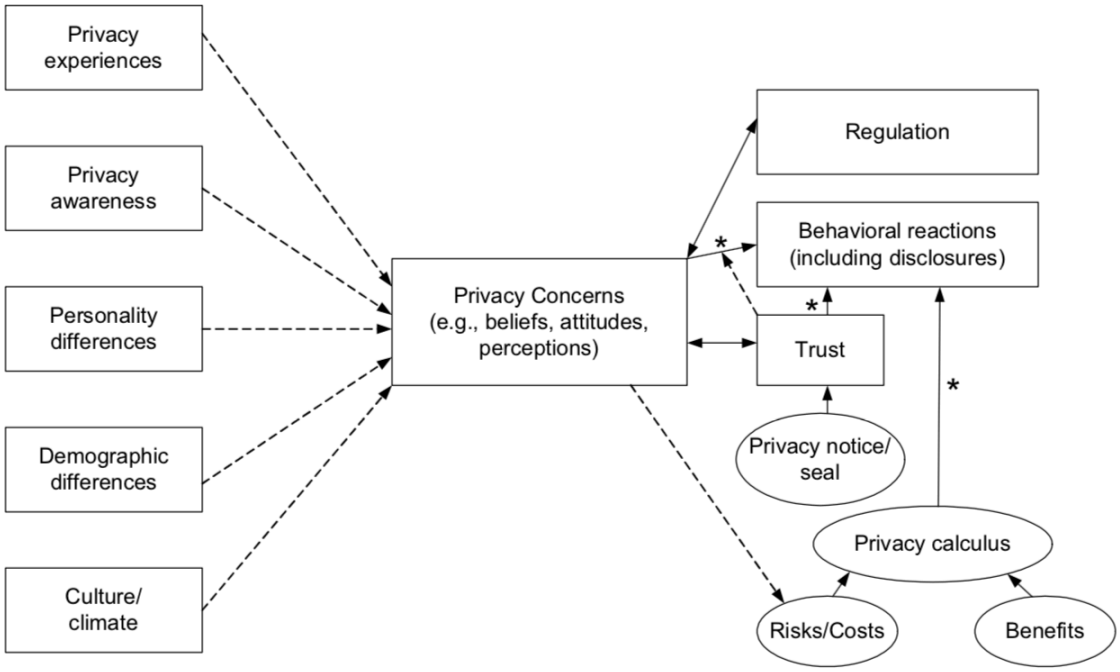

Abbildung 1: APCO-Modell (Smith, Dinev, & Xu, 2011, S. 998)

Wie in Abbildung 1 zu sehen, werden die Privatsphärebedenken eines Individuums durch verschiedene Einflussfaktoren und die persönlichen Hintergründe des Individuums beeinflusst. Hierbei wirken neben demographischen Merkmalen und der kulturellen

Prägung, die eigene Persönlichkeit sowie der Erfahrungsgrad und das Bewusstsein für Privatsphäre auf die eigenen Bedenken ein. Regulierungen von außen können diese Bedenken verstärken oder abschwächen, bieten überdies hinaus jedoch auch den rechtlichen Raum in dem die Kosten-Nutzen-Abwägung stattfindet. Ein weiterer wichtiger Faktor ist das Vertrauen, welches ein Unternehmen zum Nutzer hin aufbaut und welches es im Kontext von Datenschutz in der Regel durch unternehmensseitige Datenschutzrichtlinien oder -versprechen kommuniziert wird. Das Vertrauen, beziehungsweise die Informationslage wirkt sich ebenso auf die Verhaltensreaktion und Aktion des Individuums aus, wie der Privacy Calculus. Das APCO-Modell kann als repräsentativ für den Verhaltensprozess angesehen werden, der sich bei der Nutzung eines datenbasierten Produktes vollzieht. Kritisch zu sehen ist, dass das Modell in gewisser Weise voraussetzt, dass der Nutzer sich sowohl über Risiken und Kosten informiert, als auch einen gewissen Vertrauensgrad gegenüber einem Unternehmen aufgebaut hat, um eine Abwägung vorzunehmen und sich für einen Verhaltensweg zu entscheiden (vgl. Eling, 2017, S.14, n. Dinev et al. 2015). Bei digitalen Produkten, die zum Beispiel nur mit einem Login vollwertig genutzt werden können, ist anzunehmen, dass sich der Nutzer in der Regel nicht in dem Maße informiert und eventueller Risiken der Nutzung bewusst ist. Es ließe sich auch die Annahme treffen, dass das heutige Bewusstsein für Privatsphäre und damit verbundene Bedenken geringer sind oder der Aufwand sich tiefgehend über Datenschutzrichtlinien und technologische Ausgestaltung eines digitalen Ökosystems zu informieren, zu aufwendig für den klassischen Nutzer ist. Die digitale Mündigkeit und Expertise eines Nutzers kann somit als Grundvoraussetzung gesehen werden, um eine Kosten-Nutzen-Abwägung bezüglich der eigenen informationellen Privatsphäre im Netz zu treffen. Es ist ein Phänomen und in gewisser Weise paradox, dass so viele Nutzer ihre Daten freiwillig preisgeben, um Zugriff auf einen Online-Dienst zu erhalten, obwohl sie sich bewusst sein sollten, dass sie ihre personenbezogenen Daten an Unternehmen weitergeben. Dieses Phänomen wird in aktueller medienwissenschaftlicher Literatur als das „Privacy Paradoxon“ beschrieben, welches auf das beschriebene „Privacy Calculus“ zurückzuführen ist und eine entscheidende Rolle im Online-Nutzerverhalten spielt.

3.3 Das Privacy Paradoxon

Menschen geben an, ihrer Privatsphäre einen hohen Stellenwert beizumessen, willigen jedoch relativ einfach dazu ein, ihre Daten preiszugeben, wenn ihnen ein Anreiz geboten wird (Athey, Catalini, & Tucker, 2017, S. 2). Dieses Phänomen wird das Privacy Paradoxon genannt. Wie zuvor vorgehoben ist das Bewusstsein für die eigene Privatsphäre eine wichtige Einflussgröße auf das Online-Verhalten von Individuen. Laut einer Studie der Initiative D21 (2018, S. 24 ff.) geben 65% der Befragten in Deutschland an aus

Datenschutzgründen weniger persönliche Daten ins Internet zu stellen, ebenfalls 65% ist bewusst, dass Firmen ihre Daten an Dritte weitergeben, nur 12% finden es in Ordnung, wenn sie ihre Daten im Tausch für die Nutzung eines Services preisgeben. Da das Nutzen von Online-Diensten, Messenger-Diensten oder eCommerce-Plattformen stark auf der Verwendung von personenbezogenen Daten basiert, gibt man in der Regel einen Teil seiner Privatsphäre preis, um den präferierten Service oder Service-Vorteil nutzen zu dürfen. Das Privacy Calculus beschreibt das Phänomen, seine Privatsphäre im Internet aufgrund einer Kosten-Nutzen-Abwägung für die Nutzung eines Produktes aufzugeben. Es ist besonders stark bei der Nutzung von sozialen Netzwerken, Messenger-Diensten oder Navigations-Applikationen ausgeprägt, da hier eine Vielzahl an persönlichen Informationen preisgegeben wird, um ein Produkt, beziehungsweise das volle Funktionsspektrum zu nutzen. Während in der Theorie des Privacy Calculus eine bewusste Abwägung vorgenommen wird, ist die Entscheidung ein Produkt zu nutzen beim Privacy Paradoxon meist konträr zur Einstellung gegenüber der eigenen informationellen Privatsphäre (Eling, 2017, S. 12). Individuen können also sehr starke Privatsphärebedenken haben, ändern aber nichts an ihren Privatsphäreeinstellungen oder verzichten auf die Nutzung einer Seite (Charlesworth, 2018, S. 21). Ursachen für das Privacy Paradox sind mannigfaltig, basieren oftmals auf Netzeffekten, Bequemlichkeit, Informationsasymmetrie oder zu schwachem Datenschutz und können schwer mit einer einzigen Verhaltenstheorie des Menschen metatheoretisch erfasst werden (Deuker, 2010, S. 276). So treffen beispielsweise viele Nutzer die Entscheidung Facebook zu nutzen, weil alle ihre Freunde bereits auf der Plattform angemeldet sind, sie die „kostenlose“ Nutzung der Plattform über die Preisgabe von personenbezogenen Daten stellen oder sich nicht über die Verwendung ihrer Daten durch das Unternehmen bewusst sind, beziehungsweise nicht ausreichend informiert worden sind. Ein weiterer wichtiger Faktor für das Privacy Paradox ist das Nutzererlebnis.

Die Preisgabe von personenbezogenen Daten kann das Nutzererlebnis maßgeblich verbessern. Schnelle und einheitliche Logins, kostenlose Nutzung, personalisierter Content und Vernetzung sind einige Faktoren, die datengetriebene Modellierung von Online-Angeboten unterstützen. Ebenfalls wenden Nutzer verhältnismäßig wenig Mühe auf, um ihre Privatsphäre zu schützen und verzichten beispielsweise darauf ihre Cookies zu löschen oder ihre Bewegungen zu verschlüsseln, obwohl dies ohne großen Aufwand möglich ist (Gerber, Volkamer, & Gerber, 2017, S. 142). Ein Grund hierfür kann fehlende technische Expertise der Nutzer sein, beziehungsweise zu intransparente Information durch die Verantwortlichen. Ein anderer Grund kann der hohe Stellenwert einer flüssigen User Experience für den Nutzer sein. Der digitale Mensch ist in hohem Maße an ein flüssiges Online-Erlebnis gewöhnt, sieht Vorteile in der personalisierten Aussteuerung

von Inhalten und intelligenter Vernetzung, stellt diese über gewisse Nachteile wie Profilierung oder ist sich dieser Nachteile überhaupt nicht bewusst. Da ein maßgeblicher Anteil der heutigen Kommunikation über soziale Netzwerke und Applikationen stattfindet, entscheidet sich der Großteil der Gesellschaft für die Nutzung der großen Plattformen wie Facebook und Google, obwohl sie diesen Unternehmen kritisch gegenüber stehen (Gerber, Volkamer, & Gerber, 2017, S. 156).

3.4 Die Digitale DNA – Eine Spurensuche

Der Kern der Privatsphäre eines Menschen ist heute der digitale Fußabdruck, den Internetnutzer hinterlassen, während sie sich im Netz bewegen (Charlesworth, 2018, S. 23). Um das Nutzerverhalten eines Nutzers nachvollziehen zu können, lohnt es sich auf Spurensuche zu gehen und die Datenspuren, die ein Nutzer hinterlässt, zu analysieren. Als digitale Spuren können alle Texte, Bilder, Log-Ins, Browser-Sitzungen, Klicks oder Online-Käufe angesehen werden, die der Nutzer bewusst oder unbewusst produziert und die seine „digitale Identität" bilden und sich zum Beispiel als Kundenprofil nutzen lassen (Reigeluth, 2015, S. 28). Sogenannte „Customer Journeys" sind im Zeitalter der Digitalisierung der Schlüssel, wenn es um Geschäftsmodellierung und Optimierung der operativen Tätigkeiten eines Unternehmens geht. Wie bewegt sich der Nutzer auf der Website, worauf klickt er, welche Werbung sieht er, was interessiert ihn, was lässt ihn Prozesse abbrechen, wie bewegt er sich im physischen Raum, wer zählt zu seinem Freundeskreis und vor allem welche Schritte durchläuft der Nutzer im Kaufprozess? Fragen wie diese lassen sich durch Datenspeicherung und -verknüpfung, Tracking und Ortungsdienste beantworten und lassen Unternehmen valide Entscheidungen treffen, die sich zum einen effizienzsteigernd und zum anderen positiv auf das Nutzererlebnis auswirken. Die Freigabe von Daten ist hier die Währung die Menschen für die Nutzung eines Dienstes eintauschen (Buck, Stadler, Suckau, & Eymann, 2016, S. 58 zit n. Wenninger et al. 2012). Loggt man sich beispielsweise im WiFi eines Hotels ein, willigt man häufig ein, dass persönliche Informationen und Bewegungsdaten erhoben werden, während man das WiFi nutzt (Charlesworth, 2018, S. 24).

Möchte man Spuren dieser Art nicht hinterlassen, so muss man anonym surfen oder wenn möglich die Einstellungen auf seinen Geräten so einstellen, dass keine Websites, Apps oder Programme Zugriff auf persönliche Daten haben. Selbst mit verstärktem Datenschutz wäre eine Ortung einer Person immer möglich, solange sie ein Mobiltelefon mit sich trägt, da man sich auf seinen physischen Routen von Sendemast zu Sendemast bewegt und alle Bewegungen, zumindest für den Telefonanbieter, nachzuvollziehen

wären (Weigend, 2017, S. 160). Neben GPS-basierten Ortungsdiensten, dienen oftmals Foto- und Videomaterial als Anhaltspunkt, um die Bewegungen von Menschen nachvollziehen zu können. Beispielsweise können Verkehrskameras, Überwachungskameras und andere Videokameras genutzt werden, um das Bewegungsmuster einer Person zu analysieren. Algorithmen sind heutzutage in der Lage anhand kleiner Merkmale eine Personenbestimmung möglich zu machen und somit einen Menschen immer dann zu erkennen, wenn er auf gefilmten oder fotografiertem Material auftaucht (Weigend, 2017, S. 163 ff.). Bei der Eingabe eines Suchbegriffes bei Google über den Browser eines Smartphones wird man in der Regel gefragt, ob man die Ortungsdienste aktivieren möchte, um ein verbessertes Suchergebnis zu erhalten. In den meisten Fällen verspricht dies einen großen Mehrwert, besonders dann, wenn die Ortungsdaten die Relevanz der gezeigten Inhalte für den Nutzer erhöhen. Werden diese Informationen jedoch an Dritte weitergegeben, um beispielsweise Werbung basierend auf einem Geo-Targeting auszuspielen, so kann dies für den Nutzer gegebenenfalls einen Vorteil mit sich bringen, jedoch aber auch sein Recht auf Privatsphäre verletzen. Ähnlich verhält es sich mit digitalen Anwendungen, die bisher analoge Lebensbereiche digitalisieren. So haben sich sowohl Smart Home Technologien, als auch digitale Anwendungen zur Optimierung der eigenen Gesundheit, hierunter Wearables wie Fitness Tracker, im Alltag vieler Bürger etabliert. „Durch ihre Kompatibilität mit den Kommunikationsmedien des Web 2.0 sorgen mikrosensorische Anwendungen schließlich dafür, dass sich die Privatsphäre des Einzelnen und seine körperlichen Aktivitäten und Gewohnheiten in die Kommunikationsräume der Mediennutzung im Front-End-Bereich und in die informatische Verdatung, das ist die Speicherung und Verarbeitung personenbezogener Daten im Back-End-Bereich der sozialen Netzwerkseiten, verschiebt (Reichert, 2015, S. 74).“

In der Vergangenheit konnte der Nutzer auf derartige Verarbeitung seiner Daten keinen großen Einfluss nehmen. In gewisser Weise ist es eine Entscheidung die der Nutzer trifft, zu welchem Zeitpunkt er die Kontrolle abgibt, jedoch wird er in der Regel nicht über dieses Verhältnis aufgeklärt. In Zukunft soll es durch Verordnungen wie der DSGVO mehr Transparenz und mehr informationelle Selbstbestimmung geben. Um diese sensible Gemengelage zu beurteilen, ist es für Unternehmen von Nöten dem Nutzer sowohl transparent zu unterrichten, was mit seinen Daten passiert und welchen Vorteil er mit der Preisgabe dieser erwirbt.

Im folgenden Abschnitt werden Vor- und Nachteile der Datenspeicherung beschrieben, um eine fundierte Grundlage für die Bewertung von Datenschutzverschärfungen zu legen.

3.5 Vor- und Nachteile datenbasierter Online-Dienste

„Im digitalen Zeitalter stellen sich Daten als grundlegend und gegeben dar, als natürliche Ressource, als Fundament und als universelle Maßeinheit des Wissens (Reigeluth, 2015, S. 21)."

In seinem Werk „Data for the People" bezeichnet der ehemalige Chefwissenschaftler von Amazon, Andreas Weigend (2017) Daten als das neue Erdöl. Daten sind demnach als Rohstoff zu sehen, der in seiner ursprünglichen Form nicht verwendet werden kann und erst durch Verarbeitung einen Nutzwert bekommt. Die von Weigend betitelten „Datenraffinerien" wie Google und Facebook bauen in diesem Sinne Daten ab, um Wert zu schöpfen, sowohl für den Nutzer, als auch für den Erfolg des eigenen Geschäftsmodells. Betrachtet man die universelle Nutzbarkeit von Erdöl und vergleicht diese mit der heutigen Nutzbarkeit von Daten, so scheint Weigends These nicht zu wage. Die Geschäftsmodelle von Google oder Facebook funktionieren nach dem Prinzip „Dienst gegen Daten" und die meisten Nutzer scheinen dies für einen fairen Tausch zu halten (Nocun, 2018, S. 31). Daten haben in der Tat einen enormen Nutzwert und es wäre fatal zu behaupten, Unternehmen würden nur im Sinne der eigenen Wirtschaftlichkeit Daten sammeln. Viele Geschäftsmodelle basieren auf einem „Customer First" Ansatz und gerade datengetriebene Produkte haben einen enormen Mehrwert für Nutzer und Nutzerinnen. So ermöglicht sogenanntes auf Big Data basiertes „Lifelogging" menschliches Leben in Echtzeit zu erfassen und durch die Aufzeichnung von Körper-, Verhaltens- und Datenspuren, Gesundheitsmonitoring oder Leistungsvermessung im Sport oder am Arbeitsplatz (Selke, 2016, S. 3). Ein Teil der Nutzer sieht Vorteile in Personalisierung. So geben 26% der Befragten einer Studie an, dass sie es gut finden, dass Unternehmen einen individuellen Tarif auf Basis des Nutzerverhaltens anbieten (Initiative D21, 2018, S. 27). Eine Betrachtung der Vorteile von Datenspeicherung ist essenziell, um eine Verschärfung und die Notwendigkeit von Datenschutz beurteilen zu können. Marketing-Bemühungen und die Gestaltung von Websites werden von vielen Nutzern umso mehr akzeptiert, je personalisierter die Inhalte sind, was zu deutlich effizienteren Prozessen führt (Will, 2015, S. 1). Personalisierung ist heutzutage kein Ad-On oder zeichnet wenige innovative Unternehmen im Markt aus, sondern die Norm (Charlesworth, 2018, S. 33). Nicht zu verkennen sind die Vorteile von Netzeffekten, wie sie bei sozialen Netzwerken oder Messenger-Diensten wie Facebook und WhatsApp zu sehen sind. Hierbei ist jedoch auch festzustellen, dass die Nutzung dieser Dienste auf einer gewissen Alternativlosigkeit beruht, so können diese als „unverzichtbare Infrastruktur für soziale Teilhabe" (Jung, 2018, S. 349) angesehen werden.

Auf der anderen Seite stehen Gefahren, die durch die Preisgabe von persönlichen Informationen entstehen können. Auch wenn die Anonymisierung von Daten als eine

angemessene Methode zum Schutz der Privatsphäre angesehen werden kann, ist eine Identifikation einer Person bei Big Data nie ausgeschlossen (Will, 2015, S. 2). Motivieren diese Gefahren die Nutzer dazu Dienste wie soziale Netzwerke nicht zu nutzen oder ihre Privatsphäreeinstellungen strikter anzupassen, kann dies hinderlich für Geschäftsmodelle sein (Ernst, 2014, S. 59). Die Verantwortlichen müssen ihr größtes Bemühen darin investieren, dem Nutzer transparent die Vorteile und Datenschutzrichtlinien zu kommunizieren, da es bei einer einmaligen Zustimmung sehr unwahrscheinlich ist, dass der Nutzer seine Einstellungen zukünftig nochmals ändert (Ernst, 2014, S. 59). Wie die großen Erdölraffinerien haben die Hüter über die größten Datenmengen eine große Marktmacht und können den Markt kontrollieren beziehungsweise dessen Entwicklung maßgeblich mitbestimmen. Die Vorteile die ein genaues Wissen über die DNA der Nutzer für den Nutzer selbst haben kann, können auch Gefahren mit sich bringen. Zum einen können die gespeicherten personenbezogenen Daten in falsche Hände geraten oder zweckentfremdet verwendet und so der Nutzer leicht manipuliert oder überwacht werden. Zum anderen lässt sich hypothetisch sagen, dass das heutige Nutzerverhalten in all seinen Facetten so gewollt und bereits sehr stark gesteuert ist, was die ethische Frage aufwirft ob wir personalisierte Werbung überhaupt brauchen und wollen (Will, 2015, S. 2). Ein Nutzer, der nur noch den Content vorgesetzt bekommt, auf den er möglichst schnell und zustimmend reagiert, kann als zufriedener Nutzer angesehen werden, sich konform in das vorherrschende (Wirtschafts-)System eingliedern.

Zudem werden Daten in der Praxis an Dritte weitergegeben, beziehungsweise zu Zwecken verwendet, die keinen Mehrwert für den Nutzer mit sich bringen, denen er nicht zugestimmt hat oder die transparent kommuniziert wurden. Eine durchaus reale Gefahr, ist diejenige die bei der Einschätzung der Kreditwürdigkeit aufkommt. Verbindungen in sozialen Netzwerken, Freundschaften, Merkmale der Freunde, Suchanfragen oder Telefongewohnheiten können dazu führen, dass die Kreditwürdigkeit in Frage gestellt wird (Jung, 2018, S. 350). So kaufte Facebook 2010 das Patent des Unternehmens „Friendster“, welches über die durchschnittliche Bonitätsbewertung der befreundeten Mitglieder bei Facebook einen Wert berechnet, der bestimmt ob die Bearbeitung eines Kreditantrages einer Person fortgesetzt wird oder nicht (Weigend, 2017, S. 140 zit. n. Lunt 2015). Bisher hatten Nutzer keinen großen Einfluss auf oder Einblick in die Verarbeitung ihrer Daten, durch verschärften Datenschutz sollen diese Diskrepanzen aus dem Weg geräumt werden. Aus ökonomischer Sicht kann es als ineffizient angesehen werden, dass Verfügungsrechte und die Erträge aus der Nutzung von personenbezogenen Daten bisher, zumindest zu Teilen, ungeklärt geblieben sind (Dold & Krieger, 2016, S. 1). Eine Partizipation der Nutzer an den Wertschöpfungsprozessen ihrer Datenströme wird ein wichtiges Diskussionsthema in der Zukunft sein (Weigend, 2017).

3.6 Informationelle Selbstbestimmung

> „Die Teilhabe an der Gesellschaft ist zunehmend an die digitale Welt gebunden. Menschen, die sich diese nicht erschließen (können), sind zunehmend von entscheidenden gesellschaftlichen und wirtschaftlichen Entwicklungen ausgegrenzt. Ziel muss es daher sein, dass sich alle BürgerInnen, unabhängig von Alter, Geschlecht oder Bildung, selbstbestimmt und kompetent in einer digitalisierten Welt bewegen können (Initiative D21, 2018, S. 7)."

Zum Abschluss des Kapitels lohnt sich ein Rückblick auf die zuvor behandelten Begrifflichkeiten, um die Relevanz von verschärftem Datenschutz und informationeller Selbstbestimmung ableiten zu können. Personenbezogene Daten sind Informationen, die zur Bestimmung einer natürlichen Person verwendet werden können, deren Verarbeitung, aus ethischer Sicht, mit einem Blick auf das Recht auf Privatsphäre durchgeführt werden sollte. Man kann feststellen, dass die informationelle Selbstbestimmung durch eine umfassende Öffnung der informationellen Privatsphäre zu Teilen aufgegeben wurde. Durch eine fehlende, einheitliche und transparente rechtliche Grundlage wird Privatsphäre bisher nicht mehr genügend geschützt und Phänomene wie das Privacy Paradoxon verstärken die wechselseitige Nutzung von Datenströmen im Kontext von Nutzererlebnis und Geschäftsmodellierung. Wird die zuvor hervorgehobene Intransparenz von Datenverarbeitung als Grundlage genommen, so kann informationelle Selbstbestimmung im digitalen Zeitalter als zentraler Faktor für die Stärkung der Nutzerrechte angesehen werden. Wie das Recht auf Privatsphäre ist die informationelle Selbstbestimmung im Grundgesetz nach Art. 1 Abs. 1 GG des Persönlichkeitsrechtes geregelt, welcher die Befugnis „über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen" (Hornung & Herfurth, 2018, S. 152) gewährleistet. Die Überführung dieses Rechtes in das Grundgesetz ist auf das Volkszählungsurteil von 1983 durch das Bundesverfassungsgericht zurückzuführen (ebd.) Selbstbestimmung ist besonders im Fall der Nutzung von digitalen Produkten Auslegungssache. Auf der einen Seite sollte man sich der Risiken der Nutzung digitaler Dienste bewusst sein, dem gegenüber steht fehlende Transparenz über diese Risiken.

Um den Begriff der informationellen Selbstbestimmung in einen marktbezogenen Kontext zu heben, lohnt es sich den ordnungsökonomischen Ansatz heranzuziehen. Dieser stellt die Frage, „wie die formellen und informellen Regeln beschaffen sein müssen, damit sich eine Wirtschaftsordnung herausbildet, die es den Mitgliedern einer Gesellschaft erlaubt, ihre individuellen Handlungen so zu koordinieren, dass sich eine effiziente Ressourcenallokation verwirklicht (Dold & Krieger, 2016, S. 1)." Überträgt man diesen Ansatz auf personenbezogene Daten, so kann eine klare Regelung der Verfügungsrechte und ein Recht auf informationelle Selbstbestimmung als essenziell für einen effizienten

Markt angesehen werden sowie eine Grundlage für effiziente Leistungsanreize, wie der Partizipation an datenbasierten Erträgen, bilden (Dold & Krieger, 2016, S. 2). Persönliche Informationen im Internet können wie zu Beginn dieses Kapitels beschrieben als Ressource oder Wirtschaftsgut verstanden werden, die auf dem Markt für personenbezogene Daten gehandelt werden. Ein weiterer Markt, der in enger Verzahnung mit dem Datenmarkt existiert, ist der „Markt der Privatheit" (Dold & Krieger, 2016, S. 3 f.). Beide Marktseiten beeinflussen sich gegenseitig und erschaffen sowohl Kosten, für Verschlüsselungsverfahren oder Opportunitätskosten, oder Nutzen, wie informationelle Beiprodukte einer Transaktion für Unternehmen, Schutz der Privatsphäre des Nutzers oder Vertrauen in Unternehmen (Dold & Krieger, 2016, S. 4). Wie anhand des Privacy Calculus hergeleitet nimmt ein (digital kompetenter) Nutzer eine Abwägung der Kosten und des Nutzens bei einem Tauschprozess, Daten gegen Nutzung, vor. Hierbei nehmen Regulierungen, anfallende Kosten und Risiken aber auch bereits erworbener Nutzen, zum Beispiel Vertrauen, eine Einflussgröße ein. Die Komplexität und fehlende Transparenz digitaler Märkte erschwert eine beidseitig zufriedenstellende Tauschhandlung. Nur ein vollends kompetenter Nutzer kann eine selbstbestimmte Abwägung vornehmen. Gesetze können hier zunächst nur die Grundlage bieten, Anreize für Unternehmen, als auch für Nutzer zu setzen, in eine reziproke Austauschbeziehung einzutreten. Aus verhaltensökonomischer Betrachtung ist diese Selbstbestimmtheit bei Nutzern in der Regel zweifelhaft, da diese die Folgen der Preisgabe ihrer Daten nur schwer einschätzen können (Dold & Krieger, 2016, S. 5 zit. n. Taylor 2004). Diese Verhaltensmuster sind ebenfalls mit dem zuvor geschilderten Privacy Paradoxon in Verbindung zu bringen. Hieraus kann geschlussfolgert werden, dass Unternehmen ein Umdenken bezüglich Privatsphäreschutz proaktiv mitgestalten sollten, um auf einer Vertrauensbasis weiterhin mit den Daten der Nutzer Wertschöpfung zu betreiben. Essenziell für einen höheren Grad an Selbstbestimmung der Nutzer ist neben Aufklärung und Transparenz, vor allem eine Stärkung seiner Verfügungsrechte. Die rechtliche Grundlage für eine ausgewogenere Austauschbeziehung soll nun vor allem die DSGVO in Europa bilden.

4 Datenschutz Grundverordnung (DSGVO)

„Die Aufgabe des Datenschutzrechts besteht darin, den Schutz natürlicher Personen bei der Verarbeitung ihrer personenbezogenen Daten zu gewährleisten (Hornung & Herfurth, 2018, S. 151)." Datenschutzrecht wurde bisher sowohl durch die europäische Datenschutzrichtlinie 95/46/EG (DSRL) sowie durch das Bundesdatenschutzgesetz (BDSG) und das Telemediengesetz (TMG) geregelt. Hinzu kommt die Datenschutzrichtlinie für elektronische Kommunikation, die ePrivacy-Richtlinie der europäischen Union. Erstmals wird es mit der DSGVO ein europäisches Gesetz zum Datenschutz geben, welches europaweit das Datenschutzrecht harmonisiert. Die neue Datenschutz-Grundverordnung der europäischen Union gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen (Art.2 Abs.1 DSGVO)." Überdies wird die Verordnung dann angewandt, wenn die Verarbeitung von personenbezogenen Daten in der Europäischen Union erfolgt, unabhängig davon, ob der Auftraggeber in der Union ansässig ist (Art.3 Abs.1&2 DSGVO). Der räumliche Anwendungsbereich ist also dann gegeben, wenn personenbezogene Daten in der europäischen Union erhoben werden. Dies ist u. a. dann der Fall, wenn gegenüber einer Person ein Produkt beworben wird oder das Nutzerverhalten analysiert wird, um ein Nutzerprofil zu erstellen.

Der Anwendungsbereich der DSGVO ist mithin auch dann gegeben, wenn innerhalb des räumlichen Geltungsbereiches beispielsweise Google oder Facebook auf Profiling basierte und segmentierte Zielgruppen in der Europäischen Union generieren und die Ergebnisse Werbetreibenden anbieten. Wichtig ist, dass sich das Produkt, egal ob Ware, Dienstleistung oder kostenlose Dienstleistung, an ein europäisches Publikum richtet, das Gleiche gilt für die „Beobachtung" von europäischen Nutzern (Härting, 2016, S. 58 f.). Hieraus lässt sich schließen, dass Praktiken des Online Marketings, wie Profiling oder Tracking, die im Folgenden genauer erläutert werden, sofern sie auf EU-Bürger angewendet werden, unabhängig vom Standort des Unternehmens, von der DSGVO erfasst werden. Datenverarbeitung, hierunter Datenspeicherung, Tracking, Profiling oder Websiteanalyse, wird innerhalb des territorialen Anwendungsbereichs der europäischen Mitgliedstaaten mit einer Vielzahl an neuen Datenschutzrechtsverschärfungen versehen. Eine Verarbeitung ist laut Artikel 6 Absatz 1 DSGVO nur dann rechtmäßig, wenn einer der folgenden Bedingungen erfüllt ist:

> a) Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;

b) die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen;
c) die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt;
d) die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen;
e) die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;
f) die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

Diese Grundprinzipien des Datenschutzes gelten als Grundlage für weitere zentrale Bestandteile der DSGVO. Neben der Stärkung der Rechte der betroffenen Personen durch Informationspflichten und Verpflichtungen zur technischen Ausgestaltung von digitalen Produkten und Online-Diensten, wird es ebenfalls Neuerungen im Bereich Einwilligung und Haftung geben. Zunächst werden die Bestandteile, Transparenz, Informationspflicht sowie Privacy by Design und Privacy by Default im Kontext informationeller Selbstbestimmung betrachtet, bevor Neuerungen zum Thema Einwilligung und Haftung hinzugezogen werden, um eine Prognose für den zukünftigen Einsatz von Opt-In-Verfahren geben zu können. Abschließend werden die Rechte des Nutzers und die im Rahmen der DSGVO angestrebte Stärkung dieser hervorgehoben, um eine umfassende Grundlage für eine folgende Interessensabwägung zu bilden.

4.1 Transparente Information

Transparenz ist ein wichtiger Faktor im Datenschutzkontext. „Ohne Transparenz wird die betroffene Person faktisch rechtlos gestellt (Hornung & Herfurth, 2018, S. 159 zit n. Roßnagel et al. 2001).“ Bereits 1983 hob das Bundesverfassungsgericht die große Bedeutung des Transparenzprinzips hervor. „Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß (Hornung & Herfurth, 2018, S. 159 zit. n. Bundesverfassungsgericht 1983).“ Die Gesetzesgrundlagen, die damals aufgrund dieser wichtigen Grundsatzentscheidung des BVerfG geschaffen worden sind, sind spätestens im Zeitalter digitaler und datenbasierter Geschäftspraktiken nicht mehr zeitgemäß bzw. nicht ausreichend, um die nötige Transparenz für den Nutzer zu gewährleisten. Einer zentralen Überarbeitung durch die DSGVO unterliegen die Informationspflichten, die die Verantwortlichen, also Unternehmen, Websitebetreiber und andere Verarbeiter,

gegenüber dem Nutzer haben. So ist der Verantwortliche dazu angehalten, dem Nutzer auf präzise, transparente, leicht zugängliche und einfach formulierte Art und Weise, spätestens innerhalb eines Monats, alle Informationen mitzuteilen, die sich auf die Verarbeitung von personenbezogenen Daten beziehen (Art. 12 Abs.1-3 DSGVO). Unter diese Informationen fallen neben der Auskunft über die Kontaktdaten des – von größeren Unternehmen – zu bestimmenden Datenschutzbeauftragten des Verantwortlichen, die Zwecke der Verarbeitung, die berechtigten Interessen, Auskunft über die Weitergabe an Dritte, die geplante Dauer der Speicherung der Daten sowie Rechte für die betroffene Person, unter diesen das Recht auf Löschung, Berichtigung und Einschränkung der Verarbeitung (Art.13 Abs.1-2 DSGVO). Die Informationspflicht gilt laut Artikel 14 DSGVO auch für Daten, die von den Verantwortlichen nicht selbst erhoben, jedoch gespeichert wurden und muss in diesem Fall auch die Herkunft der Daten beinhalten (Art.14 Abs.1-3 DSGVO). Wurden dem Nutzer die Informationen bereits vorher zur Verfügung gestellt, so müssen diese ihm nicht nochmals zur Verfügung gestellt werden, ändert sich jedoch der Zweck der Verarbeitung, muss dieser ebenfalls transparent mitgeteilt werden.

Hier könnte ein transparentes Opt-In-Verfahren auf einer Website oder in einem digitalen Ökosystem Verwendung finden, um für eine rechtliche Absicherung auf Seiten der Verantwortlichen vorzusorgen. Bereits im BDSG wurde eine Informationspflicht festgehalten, die DSGVO bringt hier jedoch eine Verschärfung mit sich. Generell ist anzunehmen, dass durch die hohen festgelegten Strafmaße, die konkreter im Folgenden genannt werden, eine rechtstreuere Umsetzung der Pflichten sowie einer Nennung dieser in den jeweiligen Datenschutzbestimmungen die Folge sein wird. In der Tat sind einige Regelungen bezüglich Informationspflichten vollständig neu, unter anderem die über das Widerrufsrecht bei Einwilligung, Informationen über berechtigtes Interesse und Speicherdauer und der Hinweis auf die Betroffenenrechte, hier speziell auf das Recht auf Löschung und Berichtigung (Härting, 2016, S. 18). Bei sogenannten automatisierten Einzelfallentscheidungen, hierunter Profiling, muss ebenfalls auf die Bildung eines Profils und auf die zugrundeliegende Logik hingewiesen werden (ebd.). Für Online-Marketing Prozesse gibt es hier also Änderungen, auf die durch Einwilligungsverfahren und transparente Offenlegung der genannten Information reagiert werden kann. Es ist sehr stark davon auszugehen, dass die Informationspflicht auch für das Setzen von Cookies zählt, da diese laut DSGVO als personenbezogene Daten behandelt werden (Intersoft Consulting, 2018). Generell wird die Transparenz sehr stark vorangetrieben und die neuen Informationspflichten könnten dazu führen, dass der Nutzer in Zukunft ein besseres Verständnis über die Verarbeitung seiner Daten erhält. Offen bleibt, wie einfach verständlich diese Auskunftsform aussehen wird und ob Nutzer sich aktiv informieren und intensiver mit dem Datenschutz beschäftigen werden. Welche Auswirkungen hat also die erhöhte

Transparenz auf Phänomene wie das Privacy Paradoxon und wird es wirklich mehr informationelle Selbstbestimmung geben. Die in der DSGVO neu verankerten Regelungen zur technischen Ausgestaltung, „Privacy by Design“ und „Privacy by Default“ sollen die Nutzerrechte und informationelle Selbstbestimmung ebenfalls stärken.

4.2 Privacy by Design und Privacy by Default

Im Rahmen der DSGVO führt die EU flächendeckende Regelungen ein, die Unternehmen und Websitebetreiber dazu verpflichten, bereits in der Produktentwicklung den Schutz der Privatsphäre zu beachten (Art.25 DSGVO). Sowohl „Privacy by Design“ als auch „Privacy by Default“ sind zentrale Diskussionsthemen, die seit den 70er Jahren im Kontext von Datenschutz diskutiert werden und bereits 1995 in der alten Datenschutzrichtlinie 95/46/EG der EU festgehalten wurden (Intersoft Consulting, 2018). „Laut Erwägungsgrund 46 dieser Richtlinie müssen bereits zum Zeitpunkt der Planung eines Verarbeitungssystems technische und organisatorische Maßnahmen (TOMs) getroffen werden, um insbesondere die Sicherheit der Daten zu gewährleisten (Intersoft Consulting, 2018).“ Unternehmen müssen also Datenschutzvorkehrungen in ihre Produktentwicklung technisch integrieren, um den Anforderungen der Gesetzesgrundlage gerecht zu werden. In Artikel 25 DSGVO ist „Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen“ nur für alle EU-Mitgliedsstaaten geregelt. Hierbei wird zwischen Privacy by Design in Absatz 1 und Privacy by Default in Absatz 2 unterschieden. Laut Artikel 25 Absatz 1 DSGVO muss der Datenverarbeiter unter Berücksichtigung des Stands der Technik organisatorische Maßnahmen zum Zeitpunkt der Planung und der Verarbeitung treffen, die die Rechte von natürlichen Personen schützen und Datenschutzgrundsätze wie etwa Datenminimierung und zweckgebundene Verarbeitung von personenbezogenen Daten umsetzen sollen.

Datenschutzfreundliche Voreinstellungen, wie sie dann vorgesehen sind, sollen ein Maximum an Privatsphäre gewährleisten und nicht selbstständig vom Nutzer vorgenommen werden müssen (Voigt & Bussche, 2018, S. 82). Hieraus ergibt sich, dass der Verantwortliche die zu implementierende Technikgestaltung an den Datenschutzgrundsätzen aus Artikel 5 DSGVO ausrichten muss, hierunter Rechtmäßigkeit, Transparenz, Zweckbindung, Datenminimierung, Richtigkeit und Integrität (Art. 5 Abs. 1 a-f DSGVO). Diese Verpflichtung kann jedoch einige Zielkonflikte mit sich bringen, da beispielsweise die Datenrichtigkeit durch eine Vergrößerung der Datenbasis verbessert werden kann, eine solche Implementierung jedoch nicht dem Prinzip der Datenminimierung gerecht wird (Härting, 2016, S. 31). Privacy by Default kann also als mit Datenschutz durch

Technikgestaltung übersetzt werden und würde beispielsweise eine App-Entwickler dazu verpflichten seine Plattform datenschutzkonform zu konzipieren und umzusetzen. In diesem Punkt wird sehr viel Proaktivität der verantwortlichen Unternehmen und Websitebetreiber gefordert sein. Ob eine solche Proaktivität und ein striktes Einhalten der technischen Bestimmungen in irgendeiner Weise zertifiziert wird oder ob Verstöße zu Präzedenzfällen führen bleibt abzuwarten.

Privacy by Default wiederum befasst sich mit den Voreinstellungen von Online-Diensten, hierunter beispielsweise Browservoreinstellungen. Diese sollen nach Artikel 25 Absatz 2 DSGVO künftig so voreingestellt sein, dass die Verarbeitung personenbezogener Daten so gering wie möglich gehalten wird, also nur die Daten verarbeitet werden, die der Zweckmäßigkeit entsprechen. Hierbei müssen ebenfalls die Datenschutzgrundsätze aus Artikel 5, wie die Integrität oder Transparenz gegeben sein, primär geht es hier aber um die Datensparsamkeit, also Datenminimierung, Speicherdauer, Zweckbindung und Zugriffsbeschränkungen für Dritte (Härting, 2016, S. 32). Wichtig werden die Verpflichtungen zu Privacy by Design und Privacy by Default dann, wenn es zu einem Urteil bezüglich einer Datenpanne käme, da hier eine dokumentierte Einhaltung der Regelungen zu erheblichen Vorteilen führen kann (ebd.).

4.3 Einwilligung, Kopplungsverbot und Opt-In-Verfahren

Ein Thema, dass für alle Verantwortlichen von großem Interesse ist, ist das der Einwilligung und der damit verbundenen Regelungen, wie dem Kopplungsverbot und dem Widerrufsrecht. Wie zu Beginn des Kapitels hervorgehoben wurde, ist eine Verarbeitung von personenbezogenen Daten dann rechtmäßig, wenn die betroffene Person ihre Einwilligung für einen bestimmten Zweck gegeben hat (Art. 6 Abs.1 a DSGVO). Es stellt sich nun die Frage, ob eine Einwilligung überhaupt notwendig ist und wenn ja wann, wie weit eine Einwilligung greifen und woran sie gebunden sein darf. Grundlegend ist zu sagen, dass die Einwilligung als die sicherste Grundlage für die Datenverarbeitung angesehen werden kann, da die betroffene Person so ein Selbstbestimmungsrecht ausüben kann (Härting, 2016, S. 88). Sie kann also als Schlüssel zur informationellen Selbstbestimmung ausgelegt werden. Nutzt man als Datenverarbeiter nun ein Einwilligungsverfahren, so sind durch die DSGVO deutlich erhöhte Anforderungen an die Wirksamkeit von Einwilligungen zu erwarten (ebd.). So muss der Verantwortlich in der Lage sein, nachzuweisen, dass die betroffene Person ihre Einwilligung gegeben hat, ebenfalls muss das Einwilligungsverfahren in verständlicher Form und leicht zugänglicher Form übermittelt werden (Art. 6 Abs. 1-2 DSGVO). Einwilligungen zur Datenverarbeitung sind nur dann gültig, wenn die Verarbeitung nicht gegen die Grundprinzipien der Verordnung

verstößt. Ebenfalls hat die betroffene Person das Recht die Einwilligung jederzeit zu widerrufen und muss ebenfalls über dieses Recht aufgeklärt werden (Art. 6 Abs. 3 DSGVO).

Weiterhin besteht das Kopplungsverbot, welches besagt, dass nur die Daten verarbeitet werden dürfen, welche zu Erfüllung des Vertrages notwendig sind. Grundlegend muss keine Einwilligung zur Datenverarbeitung eingeholt werden, solange nur Daten verarbeitet werden, die zur Erfüllung des Vertrages erforderlich sind. Es dürfen in diesem Zusammenhang jedoch auch keine weiteren Daten erhoben werden, beziehungsweise darf die vertragliche Leistung nicht von einer Einwilligung in die Verarbeitung von personenbezogenen Daten abhängig gemacht werden, die nicht in direktem Zusammenhang mit der Erfüllung der Leistung stehen (Härting, 2016, S. 95). Das Kopplungsverbot wurde bereits nach § 28 Abs. 3b BDSG so ausgelegt (Petrlic & Sorge, 2017, S. 422 f.). Es dürfen beispielsweise keine Newsletter mehr verschickt werden, nur weil man ein Produkt kauft oder im Sinne der Datenminimierung Daten nicht für spätere Zwecke gespeichert werden. Bisher gab es nur punktuell Kopplungsverbote, durch die DSGVO wird es allgemeine Kopplungsverbote geben, eine Einwilligung bei Verstoß gegen das Kopplungsverbot wäre unwirksam. Besonders interessant ist die Beurteilung des Kopplungsverbotes bei den großen Ökosystemen von Google und Facebook, da hier bei einem flächendeckenden Login nicht klar ist, für welche Anwendung innerhalb des Ökosystems man seine Daten preisgibt.

Weiterhin müssen Einwilligungserklärungen klar und verständlich sein und dürfen laut DSGVO Bestandteil der AGBs sein, müssen hier jedoch deutlich hervorgehoben werden (Härting, 2016, S. 89). Ebenfalls sind sie durch einen einfachen Mausklick, also durch Anklicken einer Klickbox, Einwilligung per Mail, mündlich, schriftlich oder sogar durch Browsereinstellungen zulässig, hingegen nicht zulässig wäre ein Opt-Out, also das Entfernen eines bereits vorausgewählten Häkchens (Härting, 2016, S. 89 ff.), wie es in Deutschland bisher häufig Praxis war. Ein Opt-In per Browsereinstellung ist als Alternative zu einem Pop-Up-Banner oder Cookie-Banner zu sehen, hier geht es nicht um Browservoreinstellungen, beziehungsweise dürften diese nicht gegen die Verpflichtungen durch Privacy by Default verstoßen. Da Cookies nun strenger als personenbezogene Daten behandelt werden, ist auch hier ein Trend zum Opt-In zu erwarten, was zu einem inflationären Einsatz der Cookie-Banner führen kann und sich somit negativ auf das Nutzererlebnis auswirken würde (Härting, 2016, S. 91). Einige Marktteilnehmer wie Google führen bereits einen Opt-In ein und andere verantwortliche Unternehmen ziehen bereits nach und integrieren mit Inkrafttreten der DSGVO vermehrt Cookie-Banner auf ihren Websites. Eine klare Verpflichtung zum Einholen eines Opt-Ins gibt es also laut DSGVO

nicht, jedoch ist ein Opt-Out nun nicht mehr ausreichend. Ein Opt-In muss zweckgebunden sein und ist dem Kopplungsverbot unterlegen. Viele erwarten, dass mit der Überarbeitung der ePVO der Opt-In für jegliche Form der Datenverarbeitung eingeholt werden muss. Festzuhalten ist, dass durch die DSGVO nicht jegliche Form der Datenverarbeitung zustimmungspflichtig wird, im Vordergrund steht die Stärkung der Betroffenenrechte, die im Folgenden genauer erläutert werden.

4.4 Stärkung der Rechte der betroffenen Person

Weitreichende Neuerungen bringt die DSGVO im Bereich der Betroffenenrechte mit sich. Es ist damit zu rechnen, dass mit Inkrafttreten der Verordnung empfindliche Bußgelder auf die Verantwortlichen zukommen, sobald die Betroffenenrechte verletzt werden (Härting, 2016, S. 163). Natürliche Personen haben neben dem Recht auf Auskunft, Löschung und Sperrung nun auch das Recht auf Zugriff und Datenübertragbarkeit, in diesem Sinne also eine weitreichend gestärkte Kontrolle über ihre Daten und damit mehr Selbstbestimmung. Das Recht auf Auskunft wurde bereits in § 34 Abs. 1 Satz 1 BDSG geregelt und verpflichtete den Verantwortlichen neben den gespeicherten Daten, die Herkunft, die Empfänger einer möglichen Weitergabe sowie den Zweck der Speicherung preiszugeben (Härting, 2016, S. 164). Neu in der DSGVO sind die Auskunftspflichten über die geplante Speicherdauer, die Rechte auf Berichtigung, Löschung, Einschränkung der Verarbeitung und Widerspruch, Logiken und Auswirkungen hinter automatisierten Einzelentscheidung wie Profiling und Datentransfers in Drittländer (Art. 15 Abs. 1-2 DSGVO). Das Auskunftsrecht wird nun ebenfalls durch das Zugriffsrecht erweitert, welches regelt, dass der Verantwortliche der betroffenen Person eine Kopie der verarbeiteten Daten zur Verfügung stellt, außer dieser Zugriff würde Rechte und Freiheiten anderer Personen, Geschäftsgeheimnisse oder auch das Urheberrecht beeinträchtigen (Härting, 2016, S. 166 f.). Das Recht auf Auskunft wurde demnach gestärkt, da sowohl die auskunftspflichtigen Daten erweitert wurden, als auch das Zugriffsrecht eingeführt wurde.

Die Stärkung der Betroffenenrechte wird ebenfalls durch eine Überarbeitung des Rechts auf Löschung beeinflusst. Bisher waren Unternehmen nur dann zur Löschung verpflichtet, wenn die Speicherung der Daten unzulässig war, ihre Richtigkeit nicht bewiesen werden konnte, sie für den Zweck der Speicherung nicht mehr erforderlich sind oder die Dauer der Speicherung unzulässig ist (Härting, 2016, S. 169). Dies waren Löschpflichten, an die sich Unternehmen zu halten hatten, welche durch die DSGVO nun zu einem Recht der betroffenen Person, zum Recht auf Löschung umformuliert wurden. In diesem Sinne müssen Daten durch den Verantwortlichen dann gelöscht werden, wenn die betroffene Person dies verlangt und entweder die Daten für den Verwendungszweck nicht

mehr notwendig sind, die betroffene Person ihr Widerspruchsrecht auf die Einwilligung oder die Verarbeitung geltend macht, die Verarbeitung unrechtmäßig ist oder die Löschung einer rechtlichen Verpflichtung nachkommt (Art. 17 Abs. 1 DSGVO). Besonders wichtig für journalistische Tätigkeiten sind die Ausnahmen von Löschungsansprüchen, die eine Verarbeitung im Sinne des Rechts auf freie Meinungsäußerung und Information, des öffentlichen Interesses, von wissenschaftlichen oder historischen Forschungszwecken und zur Ausübung von Rechtsansprüchen von diesem Recht befreien (Härting, 2016, S. 172). Komplett neu ist das Recht auf Datenportabilität oder auch Datenübertragbarkeit, welches regelt, dass Daten die unmittelbar von der betroffenen Person stammen und auf Basis einer Einwilligung zur Verarbeitung oder Erfüllung eines Vertrages erhoben und verarbeitet wurden, in strukturierter und maschinenlesbarer Form an den Betroffenen oder einen anderen Verantwortlichen herausgegeben werden müssen (Art. 20 Abs. 1 DSGVO). Diese Regelung bedeutet also, dass es beispielsweise möglich ist Daten eines Anbieters zu einem anderen Anbieter mitzunehmen, sozusagen die Plattform zu wechseln. Wettbewerbliche Vorteile durch Lock-In-Effekte und andere Vorteile, die an eine langfristige Nutzung einer Plattform oder eines Anbieters gebunden sind, unterliegen durch diese neue Rechtslage einer Schwächung. Abzuwarten bleibt, ob die Verantwortlichen in kürzerer Zeit eine einheitliche, strukturierte und maschinenlesbare Form der Datendokumentation verwenden, die problemlos von einem Konkurrenten ohne größere Aufwände genutzt werden kann.

Es lässt sich als Zwischenfazit ziehen, dass die DSGVO besonders die Betroffenenrechte stärkt und durch Informationspflichten für mehr Transparenz und durch Vorgaben zur technischen Ausgestaltung wie Privacy by Design und Privacy by Default für eine gestärkte digitale Selbstbestimmung sorgt. Neurungen zur Tragweite von Einwilligungen sorgen nicht direkt für Umwälzungen, motivieren jedoch die Verantwortlichen zur Proaktivität und Innovation im Bereich Opt-In. Wie genau sich die DSGVO auf Online-Marketing Prozesse auswirkt und welche Umwälzungen in Zukunft durch die ePVO und weitere Verschärfungen zu erwarten sind, wird im folgenden Kapitel tiefgehender behandelt.

5 Auswirkungen verstärkten Datenschutzes auf das Online Marketing und das eBusiness

Änderungen am Datenschutzrecht, wie sie im Mai 2018 durch die DSGVO europaweit vorgenommen wurden, stellen die digitale Branche und speziell Unternehmen, die ihre Geschäftsprozesse datenbasiert aussteuern, vor immense Herausforderungen. Wie in Kapitel 3.1 beschrieben lässt die Eingrenzung des Personenbezugs erheblichen Spielraum. Die DSGVO weist stellenweise eine normative Unschärfe auf, die es Unternehmen erschwert, für datenbasierte Praktiken, wie verhaltensbasierte Werbung oder personalisierte Aussteuerung von Inhalten, klare Verarbeitungsvorgänge abzuleiten (Voigt & Bussche, 2018, S. 311). Im Kontext von Big Data und den damit verbundenen Wertschöpfungsprozessen, ist ein genaues Wissen über datenbezogene Praktiken im digitalen Kontext erforderlich. Der Handel von persönlichen Daten und Nutzerprofilen sowie deren Auswertung und Verwertung sind zentraler Bestandteil der Geschäfts- und Monetarisierungsmodelle vieler digital agierender Unternehmen (Buck, Stadler, Suckau, & Eymann, 2016, S. 58). In diesem Kapitel soll speziell auf die dem Online Marketing nahestehende Verfahren wie Tracking und Profiling eingegangen werden, um eine Grundlage für die qualitative, methodische Untersuchung des Datenschutzrechts im wirtschaftlichen Kontext zu schaffen. Hierbei sollen die Zusammenhänge zwischen datenbasierten Praktiken und Datenschutz aufgezeigt werden sowie auf die Rolle eingegangen werden, die die führenden Unternehmen in der Online- und Tech-Industrie in diesem Kontext einnehmen.

5.1 Der Wert von Daten für das Online Marketing

Daten haben für das Online-Marketing einen enormen Wert. Im klassischen Display Advertising werden Werbebanner oder Videos in Umfeldern platziert, in welchen man seine Zielgruppe erwartet. Greift man jedoch auf personenbezogene Daten zurück, so wird von „Programmatic Advertising“ gesprochen. „Je bessere und umfangreiche Daten zur Verfügung stehen, desto zielgenauer können potenzielle Kunden identifiziert und durch Werbung angesprochen werden (Kamps & Schetter, 2018, S. 90).“ Hierbei unterscheidet man zwischen First-, Second- und Third-Party-Daten. First-Party-Daten sind die Daten, die auf der eigenen Website entstehen, wenn Nutzer sich auf der Seite bewegen, Informationen eingeben, Nutzerprofile anlegen, Produkte in den Warenkorb legen oder einen Kaufprozess durchlaufen (ebd.). First-Party-Daten sind aus dem Grund so wertvoll, weil sie in der Regel exklusiv sind und sich dafür nutzen lassen, die eigene Oberfläche zu optimieren und die eigenen Kunden wieder zu erreichen. Es ist eine wichtige Information

für Werbetreibende, speziell im eCommerce, wo sich der Nutzer im Sales Funnel befindet (Charlesworth, 2018, S. 17), wie weit er noch von einem Kauf entfernt ist. Second-Party-Daten sind identisch mit First-Party-Daten, werden aber von einem externen Unternehmen bezogen und dienen wie die anonymisierten Third-Party-Daten oftmals dazu, die eigene Reichweite zu erhöhen und neue Nutzer auf die Seite zu lenken (Kamps & Schetter, 2018, S. 90 f.). Facebook beispielsweise nutzt die eigenen First-Party-Daten, um seinen Werbekunden segmentierte Zielgruppen anzubieten. Bietet Unternehmen also die Möglichkeit an, genau die Nutzer zu erreichen, die sich durch die gewünschten Merkmale auszeichnen. Ebenfalls ermöglicht Facebook die Ansprache sogenannter statistischer Zwillinge, in dem sie First-Party-Daten ihrer Werbekunden mit den eigenen Nutzerdaten „matchen“ und somit nur die Facebook Nutzer angesprochen werden, die den tatsächlichen Kunden des Unternehmens sehr ähnlich sind. Die verwendeten Daten dürfen hierbei nur anonymisiert verwendet werden und nicht personenbezogen gespeichert werden. Werden Daten in Cookies gespeichert, welche einem Websitebetreiber dabei helfen, einen Nutzer wiederzuerkennen und seine Präferenzen zu speichern, gelten nach EU-Recht bestimmte Regeln, an die man sich halten muss.

Cookies sind Textdateien. Sie können vom Web-Server auf den Endgeräten der Nutzer, auf dem Server selbst und im JavaScript gespeichert werden und sorgen dafür, dass man beispielsweise auf einer Seite eingeloggt bleibt, Inhalte personalisiert ausgespielt werden oder alte Suchanfragen gespeichert bleiben (European Commission, 2018). Ohne Cookies wäre die Realisierung eines Online-Shops nicht wirklich möglich, da beispielsweise dem Warenkorb zugefügte Produkte nicht dem einzelnen Nutzer zugeordnet werden könnten (Petrlic & Sorge, 2017, S. 236). Die Verwendung von Cookies war nach alter Gesetzgebung durch BDSG und TMG bereits zustimmungspflichtig und die meisten Websites haben sich das Opt-In durch die bekannten Cookie-Banner eingeholt. Durch einfaches Löschen des Puffer-Speichers (Cache) im Browser ist man in der Lage, alle Cookies von seinem Gerät zu löschen, hatte somit bereits vor der DSGVO die Möglichkeit selbstbestimmt mit Cookie-Daten umzugehen. Wie bei Daten wird auch bei Cookies zwischen verschiedenen Arten unterschieden. Hierbei wird zwischen Session Cookies, welche gelöscht werden, wenn der Nutzer die Seite verlässt, und Persistent Cookies unterschieden. Persistent Cookies werden für einen gewissen Zeitraum auf dem Endgerät des Nutzer gespeichert und ermöglichen eine Widererkennung des Nutzers bei zukünftigen Besuchen (European Commission, 2018). Ebenfalls wird zwischen First Party Cookies, die vom Server der besuchten Seite gespeichert werden, und Third Party Cookies unterschieden, die von einem externen Server gespeichert werden (ebd.) Einfache Session Cookies dürfen immer ohne Einwilligung des Nutzers gesetzt werden, während Persistent Cookies und Third Party Cookies informations- und einwilligungspflichtig sind

(ebd.). Nach § 15 Abs. 3 TMG ist der Einsatz von Cookies zur pseudonymisierten Profilbildung erlaubt. Nutzer haben jedoch das Recht, sich gegen dieses Verfahren durch einen Opt-Out zu entscheiden (Petrlic & Sorge, 2017, S. 433). In der europäischen ePrivacy-Richtlinie von 2009 wird währenddessen von einem Opt-In ausgegangen, der Nutzung von Cookies muss also explizit zugestimmt werden (ebd.). Der Umgang mit Cookies als personenbezogenen Daten wird mit der DSGVO noch einmal strenger behandelt. Die in Deutschland gängige und im TMG festgehaltene Opt-Out Lösung wird nicht mehr gültig sein, da hier der Nutzer erst seine Einstellungen ändern muss, um die Einwilligung „rückgängig" zu machen. Ebenfalls müssen durch die DSGVO Cookies und Mobile Identifier aus den Datensätzen der Unternehmen gelöscht werden, wenn sie den rechtlichen Rahmen zeitlich oder zweckgebunden überschreiten (Art. 5. Abs. 1 DSGVO). Wie bereits im Kapitel über personenbezogene Daten erläutert wurde, werden Cookies nicht mehr als anonym betrachtet und daher rechtlich anders behandelt.

5.2 Tracking

„Tracking bezeichnet das Verfolgen von Nutzeraktivitäten (im Web) und das Bilden von Nutzungsprofilen (Petrlic & Sorge, 2017, S. 234)." Tracking bezeichnet weiterhin das Erstellen von Bewegungsprofilen der Nutzer sowie die Erhebung von Statistiken über die Websitenutzung. Diese Profile und Statistiken dienen zum Beispiel Werbetreibenden dazu, möglichst genau zu wissen, wo ihre (potentiellen) Kunden anzutreffen sind. Bei einem Aufruf einer Website ohne Cookies, kann der Webserver nur die Daten speichern, die ihm der Browser und die IP-Adresse des Aufrufers übermitteln. Hier wird nur die Anfrage, der verwendete Browser, die bevorzugte Sprache und gegebenenfalls die zuvor besuchte Website übermittelt, eine Wiedererkennung des Nutzers ist erst über Tracking-Verfahren, wie Cookies oder Pixel möglich (Petrlic & Sorge, 2017, S. 234 f.). Zu Beginn dieses Kapitels wurde bereits umfassend erklärt, welche unterschiedlichen Cookies bei Websiteaufrufen gesetzt werden und welchen Zweck diese haben. Cookies sind jedoch nicht das einzige technische Verfahren, welches die Erkennung und Verfolgung von Nutzern ermöglicht. Ein weiteres Verfahren sind Trackingpixel, unsichtbare Einbettungen auf einer Website, die meist über JavaScript-Code Nutzerbewegungen messen (Petrlic & Sorge, 2017, S. 242). Tracking-Pixel dienen dazu, wichtige Informationen über die Nutzeraktivitäten auf einen externen Server zu laden. Hierzu gehören Informationen auf welche Anzeigen ein Nutzer geklickt hat, bevor er beispielsweise ein Produkt gekauft hat. Tracker wie diese sind für die Umsatz-Attribution im eCommerce von herausragender Bedeutung, da so nicht nur der letzte Klick, sondern alle Kontaktpunkte eines Kunden bis zum Kauf mit der Transaktion in Verbindung gebracht werden können. Für die Messbarkeit von Marketing-Maßnahmen sind ebenfalls Trackingpixel von großer

Bedeutung, so werden nicht nur geklickte Werbeanzeigen erfasst, sondern auch Anzeigen, die ein Nutzer gesehen hat.

Tracking ist nach Regelung der DSGVO, im Sinne des Kopplungsverbots nur dann erlaubt, wenn es zweckgebunden ist, also in direkter Verbindung mit einer Transaktion oder einer Zustimmung zur Nutzung eines Dienstes steht. Daten dürfen nicht ohne Grund erhoben werden, um sie beispielsweise zu einem späteren Zeitpunkt nutzen zu können (Art- 5- Abs. 1b DSGVO). Ebenfalls gilt bei Cookies die „Same Origin Policy", die besagt, dass Cookies an den Ursprungsserver zurückgeschickt werden müssen und somit ein Tracking über mehrere Websites hinweg nicht möglich ist (Petrlic & Sorge, 2017, S. 237). Diese Richtlinie wird jedoch häufig dadurch umgangen, dass externe Anbieter (bspw. Werbetreibende) ihre externen Server anbinden und eigene Cookies setzen und lesen (ebd.). Verfahren wie diese sind sehr hilfreich um die Customer Journey und generell das Nutzerverhalten und Präferenzen besser zu verstehen, jedoch können sie im Datenschutzkontext kritisch gesehen werden.

5.3 Profiling

Ein zentraler Begriff, der in der DSGVO an weitreichende Regulierungen geknüpft ist, ist der des Profilings. Als Profiling wird „jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten" (Art. 4 Abs. 4 DSGVO), verstanden. Im Performance Marketing sind auf Profiling basierte Zielgruppensegmentierungen von herausragender Bedeutung, da nur so personalisierte und benutzerspezifische Werbung oder Inhalte ausgespielt werden können und damit der Streuverlust der Werbemaßnahmen möglichst geringgehalten wird. Für viele Mediaagenturen stellt diese Praktik einen zentralen Bestandteil ihres Produktportfolios dar. Unternehmen wie Facebook und Google besitzen durch ihre reichweitenstarken Produkte sehr präzise Profile von beinahe allen ihren Nutzern und verkaufen diese in der Regel pseudonymisiert an Werbetreibende und andere Interessierte. Da Profiling häufig auf einer Vielzahl an Charakteristika eines Individuums basiert und die Verarbeitung dieser Daten sehr stark in die Privatsphäre der Nutzer eingreift, wird diese Praktik zentral in der DSGVO behandelt. Beim Profiling wird in der Regel auf Big Data zurückgegriffen, also Datensätze die so viele Informationen beinhalten, dass hieraus präzise Nutzerprofile gebildet werden können. Auch wenn diese Daten pseudonymisiert sind, ist laut DSGVO dann ein Personenbezug möglich, wenn dieser z.B. durch die Kombination verschiedener Informationen möglich gemacht wird (Voigt & Bussche, 2018, S. 312). Aus diesem Grund wird dieses Verfahren neuerdings besonders

kritisch behandelt und in Artikel 22 DSGVO mit einer Sondervorschrift bedacht (ebd.). „Die betroffene Person hat das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt (Art. 22 Abs. 1 DSGVO).“ Profiling ist laut DSGVO also verboten, außer es ist an die Erfüllung eines Vertrags oder an eine Einwilligung der betroffenen Person gebunden (Art. 22 Abs. 2 DSGVO). Automatisierte Entscheidungsfindung ist hier der zentrale Begriff, der dann vorliegt, wenn eine rein automatisierte Bewertung von persönlichen Informationen einer bestimmten natürlichen Person vorgenommen wird (Voigt & Bussche, 2018, S. 241). Die Sondervorschrift gilt wohl nicht für personalisierte Werbemaßnahmen, da diese grundlegend nicht verboten sind, da sie keine Gefahr für die Freiheit und Rechte der betroffenen Person darstellen (Voigt & Bussche, 2018, S. 243). Eine Umsetzung des in Kapitel 3.5 vorgestellten Facebook Patents zur Bonitätsbewertung von bestimmten Personen in einem sozialen Netzwerk sollten demnach nicht zulässig sein, da diese Bewertung von einem automatisierten Algorithmus durchgeführt wird. Letztlich stellt sich jedoch bei Ökosystemen wie Facebook oder Google immer die Frage, wie weit der Verfügungsrahmen greift, dem man mit seinem Login und seiner Zustimmung zu der Datenverarbeitung durch diese Unternehmen aufgibt.

5.4 Die Dominanz der großen Vier

Der Netzwerkbegriff dominiert die Themen der Neuzeit und wird inflationär für jegliche Verbindungen, Strukturen und Abhängigkeiten genutzt (Ferguson, 2017, S. 31). Gerade digitale Märkte zeichnen sich stark durch Netzwerkeffekte aus, die zum einen den Nutzen jedes Einzelnen stark erhöhen, auf der anderen Seite jedoch auch natürliche Monopole für die jeweiligen Marktplattformen schaffen. Grund hierfür sind unter anderem Lock-In-Effekte, die einen Wechsel auf kleinere Plattformen für die meisten Nutzer durch hohe Wechselkosten unattraktiv machen (Dold & Krieger, 2016, S. 6). Zwar wurde durch die DSGVO ein harmonisiertes Recht auf Datenportabilität eingeführt, jedoch ist zu erwarten, dass die großen Plattformen wie Google, Facebook, Amazon oder Apple weiterhin von ihren großen Marktanteilen profitieren werden. Sie können ihre Nutzer binden und sich möglicherweise erfolgreicher auf Datenschutzverschärfungen einstellen, am Ende also weiterhin nach dem Prinzip „the winner takes it all“ agieren. Mehr als die Hälfte des Wachstums des Online-Marktes der USA konnte 2016 auf Amazon zurückgeführt werden (Galloway, 2017, S. 13). Facebook konnte seine Zahl an monatlich aktiven Nutzern von weltweit rund 1,05 Milliarden im Jahr 2012 (Facebook annual report 2012) auf fast 2,2 Milliarden Nutzer im 1. Quartal, 2018 (Facebook, 2018) steigern. Google schafft es in manchen Bereichen des Online-Werbemarktes einen Anteil von 90% zu besitzen.

Apple war 2017 mit einer Marktkapitalisierung von 794 Milliarden das größte und profitabelste Unternehmen der Geschichte (Galloway, 2017, S. 2 ff.).

Was diese vier Unternehmen gemeinsam haben, ist die Eigenschaft eines Ökosystems, welches flüssig, vorteilhaft und das Produktportfolio so breit für den Nutzer ist, dass er es kaum verlassen muss. Sie teilen sich den Markt in gewisser Weise auf, während Google den Nutzern hilft, das zu finden, was sie beschlossen haben zu kaufen, hilft Facebook den Nutzern durch intelligente Algorithmen und Machine Learning bei der Entscheidung, was sie eigentlich wollen (Ferguson, 2017, S. 416). Hierbei sind jedoch nicht die Nutzer die Kunden, sondern die Werbetreibenden (Nocun, 2018, S. 30). Kritische Stimmen bilanzieren, dass Facebook fast alles über seine Nutzer weiß und die Aufmerksamkeit der Nutzer an Werbetreibende aus der ganzen Welt verkauft (Ferguson, 2017, S. 418). Dieses Verhältnis ist in heutigen Zeiten der Werbung tatsächlich gängige Praxis und wie bereits aufgezeigt wurde, kann man sich als Nutzer mit der nötigen Kompetenz über die Risiken und Vorteile der Nutzung von „kostenlosen“ Diensten bewusst sein. Gerade am Beispiel Facebook ist jedoch zu sehen, dass mit den vielen Vorteilen der Nutzung der großen Dienste ebenfalls ein schwindender Wettbewerb einhergeht und Konkurrenten wie WhatsApp oder Instagram aufgekauft werden. Für Konkurrenten und aufstrebende Unternehmen im Digital- und Online-Werbemarkt ist es schwierig gegen das Wachstum dieser Unternehmen anzukommen. Einer WARC Studie zufolge gehen 18% der digitalen Werbeausgaben in 2017 an Facebook, ganze 44% an Google (Werner & Buttlar, 2018). Dieses Verhältnis zu regulieren, sollte von großem Interesse für die Staatengemeinschaften sein, dies ist jedoch deswegen so schwierig, da Unternehmen, die kostenlose Plattformen oder Produkte anbieten, ihren Erfolg und ihren Umsatz meistens auf Basis der großen Nutzerzahl, deren Daten und den damit verbundenen Werbeeinnahmen auf-bauen (ebd.).

Dass Facebooks Mehrwerte für Werbetreibende auch für die politische Mobilisierung genutzt werden können, sollte nicht erst seit Cambridge Analytica klar sein (Ferguson, 2017, S. 447). Es ist nur schwierig die Möglichkeiten eines solchen Netzwerks zu regulieren, ohne ganze Geschäftsmodelle und den Markt zu gefährden. Es wird sich zeigen, ob sich diese Unternehmen in Europa an die Vorschriften zur Datensparsamkeit, Richtigkeit von Daten und Zweckgebundenheit halten. So zeichnete Amazon bisher neben der Kauf- und Warenkorbhistorie ebenfalls alle Klicks auf Werbebanner, Suchanfragen und Bewegungsdaten auf der Seite seit dem ersten Login auf und das mit klarem Personenbezug, da ein Nutzerkonto im eCommerce nie pseudonym ist (Nocun, 2018, S. 50). Der endlosen Datensammlung sind sich die wenigsten Nutzer wohl bewusst und es schwierig zu ermitteln, wie weit Zweckgebundenheit ausgelegt werden kann und ab

wann Daten gelöscht werden müssten. Im Kontext dieser Arbeit stellt sich die Frage, welchen Einfluss verschärfter Datenschutz auf die dominanten Marktteilnehmer hat. Regulierungen wie die DSGVO sind sicherlich sinnvoll, jedoch lässt sich die These aufstellen, dass es die großen Unternehmen einfacher haben, sich auf diese einzustellen.

6 Lösungen zur Schaffung von Privatsphäre

In Kapitel 3.1 wurde anhand des APCO-Modells dargestellt, wie beim Privacy Calculus eine Kosten-Nutzen-Abwägung stattfindet, bei der sowohl Privatsphärebedenken als auch das Vertrauen in das Unternehmen, Kosten und Risiken der Nutzung und staatliche Regulierungen einbezogen werden. Hieraus lässt sich eine Handlungserklärung ableiten, die besagt, dass Nutzer basierend auf einer Abwägung entscheiden, ob sie einen Online-Dienst nutzen oder nicht. Das in Kapitel 3.3 untersuchte Privacy Paradoxon zeigt jedoch auch, dass viele Nutzer konträr zu ihren Privatsphärebedenken handeln und sich konsequent für die Nutzung von Diensten entscheiden, die einen Eingriff in ihre Privatsphäre ermöglichen.

Die DSGVO kann als Regulierung gesehen werden, die auf der einen Seite die Rechte der betroffenen Person stärkt, auf der anderen Seite die Verantwortlichen dazu anhält ihre Datensicherheit zu verschärfen und die Nutzer transparenter zu informieren. Wie zuvor geschildert, basieren Online-Marketing-Prozesse in großem Maße auf datenbasierter Aussteuerung. Beschriebene Opt-Out-Verfahren oder rechtliche Einschränkungen in der Verwendung von Cookies bedeuten einen Mehraufwand für Unternehmen und erschweren datenbasierte Praktiken im Online Marketing, während die Nutzer nun selbstbestimmter ihre Daten verwalten und ihre Privatsphäre schützen können. Im folgenden Kapitel wird dargelegt, welche Möglichkeiten der Nutzer selbst nutzen kann, um seine Privatsphäre zu schützen. Hierfür lässt sich zunächst die Protection Motivation Theory anführen, die einen Erklärungsansatz darstellt, welche Faktoren der Nutzer in seine Entscheidung sich zu schützen einbezieht. Demnach hat ein Mensch zwei Möglichkeiten auf eine Gefahr zu reagieren: Nichts tun oder eine Gegenaktion einleiten (Ernst, 2014, S. 59).

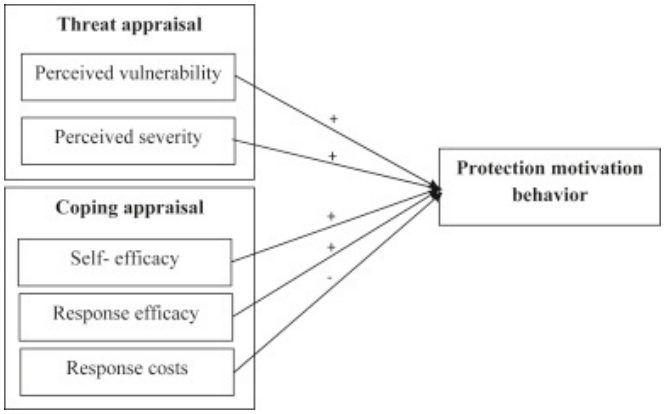

Abb. 2: Protection Motivation Theory, Science Direct (2018)

Hierbei bezieht sich die betroffene Person auf zwei Faktoren, die seine Schutzmotivation beeinflussen. Zum einen die Bedrohungsbeurteilung, bei der eine Einschätzung des Gefahrengrads vorgenommen wird, zum anderen eine Reaktionsbeurteilung, bei der sowohl die Selbstwirksamkeit, als auch die Effektivität und die eventuellen Kosten der möglichen Handlungen einbezogen werden (Ernst, 2014, S. 59). Bei der Bedrohungsbeurteilung werden sowohl negative als auch positive Folgen des Handelns einbezogen. Hieraus bildet sich die Motivation, Schutzvorkehrungen zu treffen und diese letztendlich umzusetzen. Es findet eine Abwägung statt, bei der die Risiken, das Ziel und die positiven Folgen der Handlung, den möglichen Kosten gegenübergestellt werden. Die Entscheidung, Schutzmaßnahmen bezüglich der Privatsphäre im Internet vorzunehmen, basiert auf ähnlichen kognitiven Prozessen, wie die Entscheidung einen Dienst trotz Privatsphärebedenken zu nutzen. Nutzer scheinen nicht dazu bereit zu sein, für den Schutz ihrer Daten zu zahlen, was auch auf die Komplexität informationeller Privatsphäre zurückzuführen ist (Buck, Stadler, Suckau, & Eymann, 2016, S. 55). Sie haben bisher jedoch auch wenig Mittel, um die Konditionen bei einer Datentransaktion zu verhandeln (Jentzsch, 2014, S. 795). Bisher blieb oft nur die Entscheidung zwischen einer Nutzung und einer Nichtnutzung. Die Kosten einer Nichtnutzung scheinen den meisten Nutzern zu hoch zu sein, um Schutzvorkehrungen für ihre Daten zu treffen.

Es ist ebenfalls anzunehmen, dass die Prozesse bei der Nutzung von Online-Diensten sehr schnell ablaufen und das Nutzerverhalten im Sinne des Privacy Paradoxons nicht auf einer rational nachvollziehbaren Abwägung basiert. Durch die DSGVO wurden die-Betroffenenrechte gestärkt, woraus eine gesteigerte Selbstbestimmung des Nutzers resultiert. Es ist imminent, dass Verantwortliche die betroffene Person transparent über ihre Tracking-Verfahren und Verwendungszwecke der Nutzerdaten aufklären, um trotz verschärften Datenschutzrechts nach wie vor wirtschaften zu können.

6.1 Technische Verfahren zum Schutz der Privatsphäre

Unter Einbeziehung der Nutzer- und Unternehmensperspektive werden im folgenden Abschnitt verschiedene technische Verfahren zum Schutz der Privatsphäre vorgestellt und diskutiert, um den aktuellen Horizont an Möglichkeiten für diese komplexe Thematik zu skizzieren. Hierbei wird davon ausgegangen, dass der Nutzer sich im Sinne der Protection Motivation Theory dafür entscheidet, gewisse Schutzvorkehrungen bezüglich seiner Privatsphäre zu treffen (Ernst, 2014, S. 59). Als bisher gängigstes Mittel dienen hier Consent-Verfahren, die bei der Öffnung einer Website abgefragt werden. Hier stimmt der Nutzer mit einem Opt-In der Datenverwendung durch den Websitebetreiber und ggf. Dritte zu oder er wählt den Opt-Out. Ein Opt-Out oder ein verweigerter Opt-In für First-

Party-Cookies kann bedeuten, dass einige Websites, somit auch die meisten eCommerce Websites, nicht genutzt werden können (Petrlic & Sorge, 2017, S. 237). Ein Opt-In besteht aus einem Klick und erfordert nicht zwingend eine Reflektion der Datenschutzrichtlinie. Auf einigen Websites kann der Nutzer im Bedarfsfall einzelne Anpassungen seiner Privatsphäre vornehmen, zum Beispiel welche Art von Cookies er zulassen möchte und welche nicht. Auf der einen Seite kann ein Einwilligungsverfahren als sichere Grundlage des Datenschutzes angesehen werden, auf der Nutzer selbstbestimmt über ihre Privatsphäre bestimmen können (Härting, 2016, S. 88). Auf der anderen Seite kann ein Einwilligungsverfahren auch als datenschutzunfreundlich angesehen werden, zum Beispiel dann, wenn eine Einwilligung zur Datenverarbeitung nicht notwendig wäre, jedoch trotzdem eingeholt wird und die Verarbeitung eigentlich nicht zweckgebunden ist. Das führt dazu, dass Unternehmen trotz neuer Bestimmungen zur Datenminimierung und Zweckgebundenheit, dennoch weiter Erhebungen durchführen, die für ihr Geschäftsmodell nicht essenziell sind und die im Zweifel nicht im Sinne des Nutzers sind. Das Interactive Advertising Bureau (IAB) Europe bietet ein DSGVO konformes "Transparency & Consent Framework" an, welches Unternehmen relativ mühelos ermöglicht, ein für den Nutzer transparentes Einwilligungsverfahren auf ihrer Website zu integrieren (Interactive Advertising Bureau, 2018). Die DSGVO sowie die vorgestellten Konzeptionen aus der Industrie bestärken die Annahme, dass sich der Online-Werbemarkt zukünftig durch ein „Consent Based Advertising" auszeichnet.

Ein weiteres Verfahren sind „Do-Not-Track" (DNT) Funktionen, die in den meisten Browsern auswählbar sind und die, genau wie beim Surfen im „Inkognito-Modus", Third-Party-Cookies blockieren (Petrlic & Sorge, 2017, S. 239). Technologien wie diese sorgen dafür, dass keine zielgerichtete Werbung ausgespielt werden kann, Werbung wird im Gegensatz zu AdBlocker-Technologien jedoch nicht gänzlich blockiert. Die Entwickler des Brave Browsers haben es sich zum Ziel gesetzt gewisse Verhältnisse im Netz zu reparieren. Der Brave Browser blockiert sowohl Tracker als auch Werbeanzeigen und lässt den Nutzer sogar transparent einsehen, wie viele Tracker und Werbeanzeigen blockiert wurden und wie viel Zeit der Nutzer hierdurch spart. Das Laden von Werbeanzeigen und Tracking-Verfahren verzögert den Aufbau einer Website und kostet Akkulaufzeit der Endgeräte. So verspricht der Browser, dass man so bis zu 23 US-Dollar monatlich sparen kann (Brave, 2018). Entgegen einem AdBlocker versucht der Brave Browser jedoch auch die Websitebetreiber mit einzubinden und verspricht Publishern weiterhin Einnahmen über ihre Inhalte zu erzielen, durch einen Blockchain basierten Token, mit dem Nutzer ihre präferierten Seiten „belohnen" können (ebd.). Entgegen der zuvor beschriebenen DNT-Funktion hat der Nutzer hier komplette Kontrolle über seine Privatsphäre, ohne auf Inhalte von Websites verzichten zu müssen. Ein gänzliches Umgehen von

Werbeanzeigen durch AdBlocker soll in dieser Arbeit nicht als Werkzeug für informationelle Selbstbestimmtheit und Privatsphäre der Nutzer vorgestellt werden, da diese Technologien als marktschädigend angesehen werden können. Vielmehr sollen Lösungen präsentiert werden, die sowohl den Nutzer als auch gängige digitale Geschäftsmodelle schützen und im Idealfall nicht einschränken.

Ein zentrales Ziel der Privatsphärenforschung ist es, den Wert von persönlichen Informationen zu ermitteln, der auf einem Angebots-Nachfrage-Prinzip beruhen könnte (Jentzsch, 2014, S. 795). Die OECD hat hierzu 2013 mehrere Methoden veröffentlicht, wie eine Kompensation von erhobenen Nutzerdaten, die auf einem Drittmarkt angeboten werden, auf den Nutzer zurückzuführen wären. Demnach könnten Marketingprofile, wie sie im sozialen Netzwerk Facebook angesteuert werden können, mit einem Gegenwert bewertet werden, der sich aus den Unternehmenserträgen auf die einzelnen Nutzerprofile verteilt (ebd.). Diese Überlegung ist jedoch schwer zu realisieren. Nimmt man den Gewinn von Facebook vom Jahr 2017, rund 4,268 Milliarden US-Dollar (Facebook Q4 2017 Results, S. 13), und teilt ihn durch die monatlich aktive Nutzerzahl von rund 2,129 Milliarden (Facebook Q4 2017 Results, S. 3), so würde jeder Nutzer genau zwei US-Dollar jährlich erhalten. Hier sind zwar nicht die Umsätze der Werbetreibenden mit einbezogenen, eine so schwer ermittelbare Kompensation würde aber wohl kaum die Ängste und Bedürfnisse der Nutzer bedienen können, da Informationstransaktionen wie sie bei Facebook gängig sind auf sehr komplexen Anreizstrukturen basieren (Jentzsch, 2014, S. 797). Eine weitere Lösung könnten Privacy Bots sein, welche Privatsphäre Präferenzen auf einer Website hinterlegen (Jung, 2018, S. 150). Diese technische Lösung könnte zum Beispiel durch eine Hinterlegung der Präferenzen in einem Browser vorgenommen werden. Der Nutzer kann so bestimmen, welche Informationen er preisgeben möchte und welche nicht. Solche Verfahren könnten jedoch zur Folge haben, dass gewisse Websites nicht mehr aufgerufen werden können, bzw. die eigenen Privatsphäre Präferenzen für verschiedene Websites und Dienstleistungen variieren und somit sehr aufwendig für den Nutzer zu verwalten sind.

Die MyData Bewegung, die Akteure aus Wirtschaft, Gesellschaft, Wissenschaft und öffentlichen Stellen repräsentiert, hat es sich ebenfalls zum Ziel gesetzt, den Bürgern ein Werkzeug zu geben, wie sie selbstbestimmt ihre personenbezogenen Daten erfassen und kontrollieren können. So könnte ein faires Verfahren geschaffen werden, wie Organisationen, Individuen und die Gesellschaft Daten nutzen und teilen können (MyData, 2018). MyData spricht bei ihrer Vision von Datenermächtigung und schlägt folgendes Verfahren vor. Nutzer pflegen ihre eigenen Daten, die in einer Datenquelle hinterlegt sind und auf die Datenverarbeiter zugreifen können, um beispielsweise Werbung

auszusteuern oder Websites zu personalisieren. Die Ermächtigung besteht darin, dass der Nutzer komplette Kontrolle darüber hat, welche Daten er preisgibt und wer diese verwendet, ohne zu große Einschränkungen in der User Experience zu erwarten (ebd.). Ein Hindernis für ein solches Verfahren kann die Trägheit und fehlende Kompetenz von Nutzern darstellen. Auch würden Teile der Industrie ein solches Verfahren ablehnen, da die Besitzrechte der Daten von Verarbeiter- auf Nutzerseite wechseln. Einen solchen Prozess müssten Gesetzgeber und/oder Unternehmen anstoßen, was die Frage aufwirft, ob staatliche Regulierung oder Selbstregulierung im Kontext von sehr komplexen Datenschutzfragen effektiver ist?

6.2 Staatliche Regulierung vs. Selbstregulierung

„Was das Internet angeht, hat zwar die Kommerzialisierung stattgefunden, die Regulierung aber fast überhaupt nicht (Ferguson, 2017, S. 413).“ Die Bemühungen der Europäischen Union durch DSGVO und EPVO die Privatsphäre der Nutzer stärker zu schützen und stärkere Rechte zur informationellen Selbstbestimmung umzusetzen, lassen sich aufgrund aufgezeigter Möglichkeiten und Risiken der Datenverarbeitung als angemessene Regulierung zum Schutz von personenbezogenen Daten rechtfertigen. Dem gegenüber stehen der freie Charakter des Internets sowie der globale Raum, in welchen eBusiness-Unternehmen agieren. Diese beiden Faktoren lassen ein staatliches Eingreifen als antagonistisch und eine Selbstregulierung als die angemessenere Maßnahme erscheinen (Will, 2015, S. 3). Bisher ließ sich jedoch kein angewandtes Konzept zur Selbstregulierung beobachten, welches gleichermaßen Nutzer schützt und Missbrauch verhindert (Will, 2015, S. 3). Andererseits sind zu starke staatliche Regularien auch nicht die alleinige Lösung des Problems, da eine zu starke Einschränkung der Datenverarbeitung vielleicht Daten besser schützt, jedoch auch Mehrwerte beseitigen kann. „In Zeiten zunehmender Digitalisierung werden wichtige volkswirtschaftliche Ressourcen verschwendet, wenn man an einem zu eng verstandenen Privatheits- bzw. Freiheitsbegriff festhält und immer höhere Abwehrmauern um das „private Individuum“ baut (Dold & Krieger, 2016, S. 11).“ Interessant ist auch die These, dass staatliche Regulierungen Unternehmen zur Selbstregulierung motivieren. Kritische Stimmen merken an, dass etwaige Regulierungen, wie der Verzicht Googles, keine Zielgruppen basierend auf Identität, Glaube oder sexueller Orientierung anzubieten, nicht mit Selbstregulierung in Verbindung zu bringen ist, sondern man schlichtweg nicht riskieren will, dass die Nutzer keine privaten Daten mehr preisgeben würden, sobald sie einem so privaten Targeting ausgesetzt wären (Nocun, 2018, S. 43). Facebook bietet seinen Kunden, also Werbetreibenden, sehr granulare Targeting-Möglichkeiten an, so können Unternehmen ihre Kundendaten Facebook zur Verfügung stellen, um basierend auf einem Datenabgleich

die eigenen Kunden auch auf Facebook zu erreichen, zum Beispiel mit Retargeting-Maßnahmen (Nocun, 2018, S. 100). Facebook agiert hier in einem rechtlich sauberen Bereich und auch Unternehmen holen sich teilweise die Berechtigung ihrer Kunden in ihren Datenschutzrichtlinien per Opt-In ein. Ethisch gesehen ist ein solches Verhalten von Unternehmen jedoch fragwürdig.

6.3 Wie muss Transparenz wirklich aussehen?

Das Bewusstsein für Datenschutz ist in den letzten Jahren gestiegen. Jährlich achten mehr Menschen darauf, weniger persönliche Informationen zu hinterlassen (Initiative D21, 2018, S. 24). Ebenfalls steigt die Akzeptanz für Unternehmen, die ihre Geschäftsmodelle an den Zugriff auf Nutzerdaten koppeln (Initiative D21, 2018, S. 27). Problematisch ist aber, dass es für Nutzer bisweilen sehr unüberschaubar ist, welche zunächst harmlosen Information wie und von wem verknüpft und verarbeitet werden und welche Erkenntnisse daraus gezogen werden können (Mühlichen, 2014, S. 95). In der Einleitung wurde der Appell genannt, dass Transparenz an die Stelle von versteckten Algorithmen treten solle. Algorithmische Vorgänge zeichnen sich dadurch aus, dass ihre Komplexität an Berechnungen auf Eingaben, Ausgaben oder Resultate reduziert wird, wodurch ein Raum für Unsicherheiten und Unbestimmbarkeiten geschaffen wird (Reichert, 2015, S. 23). Aufgrund dieser Intransparenz werden gesellschaftliche und politische Stimmen immer lauter, die einen Gesellschaftsvertrag für das digitale Zeitalter fordern (Danwitz, 2015, S. 581). Mit so einem Gesellschaftsvertrag kann die Europäische Union nicht dienen, mit der DSGVO versucht sie jedoch der beschriebenen Intransparenz entgegenzuwirken. Wie in Kapitel 4.1 geschildert, hält die DSGVO die Verantwortlichen dazu an, transparenter darzulegen, wie, wann und für welchen Zweck personenbezogene Daten genutzt werden. In Form von Datenschutzrichtlinien und AGB werden diese Punkte, durch die DSGVO angeregt, wohl umfassender dokumentiert und dem Nutzer zur Verfügung gestellt werden. Laut OECD können Unternehmen ihre Online-Konsumenten über Geschäftsbedingungen, Produkte aber auch über Datenschutzrichtlinien durch Pop-Ups, Videos oder Webbanner informieren, um Konsumentenbedenken zu begegnen (OECD, 2016). Es gibt Stimmen, die diese Praxis dennoch nicht als ausreichend betrachten, da Nutzer diese Richtlinien oftmals nicht verstehen oder keine Zeit oder Lust haben, sich durch Seiten voll Fachvokabular zu klicken (Wass & Kurz, 2012, S. 750 f.). So geben 58% der Deutschen an in etwa zu wissen, was Cookies sind, nur noch 21% können etwas mit dem Begriff Big Data anfangen (Initiative D21, 2018, S. 21).

Damit Nutzer gänzlich selbstbestimmt mit ihren Daten umgehen können, ist ein hohes Maß an Transparenz nötig. Ein hohes Maß an Transparenz darf aber nicht heißen, den

Nutzer mit zu vielen Informationen über seine Privatsphäre zu überfordern und einen Informationsoverflow zu provozieren. Eine Überladung an Informationen führt dazu, dass Nutzer weniger selbstbestimmt und daher verwirrter agieren (Lee & Lee, 2004, S. 177). Die in den in der DSGVO gestärkten Betroffenenrechten wie Datenportabilität, Recht auf Berichtigung, Recht auf Löschung und Datensicherheit können als geeignete Maßnahmen zu Herstellung von Transparenz angesehen werden. Wichtig hierbei ist es jedoch, dass diese Rechte in geeignete Werkzeuge übersetzt werden und dass die Daten, die bei der Ausübung dieser Rechte entstehen auch von Unternehmen genutzt werden, um ihre Produkte zu verbessern (Weigend, 2017, S. 195). Es muss Nutzern also bewusster werden, welchen Wert ihre Daten wirklich haben, was jedoch aufgrund des hohen Abstraktionsgrades des Entstehungsprozesses von Daten sehr schwierig scheint (Buck, Stadler, Suckau, & Eymann, 2016, S. 59). Dies ist besonders in der heutigen Zeit von großer Bedeutung, in der datengetriebene Anbindungen immer stärker in unseren Alltag integriert sind.

7. Empirische Methodik

Im Verlauf dieser Arbeit wurden verschiedene theoretische sowie rechtliche Inhalte beleuchtet, um eine fundierte Grundlage für die Untersuchung des Forschungsziels dieser Arbeit zu bilden. Hierbei wurde zum einen untersucht, welche Auswirkungen durch die DSGVO der Europäischen Union im Hinblick auf Online Marketing Prozesse, Nutzerverhalten und die Privatsphäre des Nutzers zu erwarten sind. Zum anderen wurde skizziert welche kognitiven Prozesse ein Nutzer im Kontext von datenbasierten Produkten oder Dienstleistungen durchläuft und welche Privatsphärebedenken er hierbei äußert und wie er auf diese reagiert. Als in der Forschung festgehaltene Phänomene wurden hier zum einen das Privacy Calculus und zum anderen das Privacy Paradoxon vorgestellt. Beide Begriffe sollen im Rahmen der empirischen Methodik ebenso beurteilt werden, wie die Relevanz und die Auswirkungen verstärkten Datenschutzes im Kontext der DSGVO. Weiterhin sollen die Erkenntnisse aus Privatsphärenforschung und Datenschutzrecht hingehend ihrer Anwendbarkeit auf den Online-Werbemarkt und die dominanten Marktteilnehmer Facebook und Google untersucht werden. Zudem sollen Einschätzungen erhoben werden, wie Nutzer zukünftig ihre digitalen Rechte selbstbestimmt einsetzen könnten. Letztendlich sollen Lösungsansätze für das komplexe Verhältnis zwischen Privatsphärebedenken, Datenschutz und dem Erfolg von digitalen Geschäftsmodellen vorgestellt werden, die sich aus den Erkenntnissen der empirischen Forschung ableiten lassen.

7.1 Forschungsdesign

Für die Realisierung der zuvor vorgestellten Forschungsziele wird eine Kombination aus zwei empirischen Methoden vorgenommen. Zum einen werden Experten auf den Gebieten Online Marketing, Advertising Technologie und Datenschutzrecht befragt, um fundierte Beurteilungen der untersuchten Schwerpunkte zu generieren. Die Befragung findet im Rahmen nicht-standardisierter (Gläser & Laudel, 2014, S. 40), qualitativer Leitfadeninterviews statt, mit dem Ziel die theoretisch erarbeiteten Inhalte zu validieren und darüber hinaus neue Erkenntnisse zu den zentralen Forschungskomponenten dieser Arbeit zu generieren. Des Weiteren wird eine Gruppendiskussion mit Nutzern digitaler Dienste durchgeführt, um die datenschutzbezogenen Phänomene des Privacy Calculus und Privacy Paradoxons zu untersuchen. Im Folgenden werden die Forschungsdesigns der gewählten Methoden vorgestellt und die Durchführung dieser protokolliert.

7.2 Experteninterviews

Da eine Befragung auf die Rekonstruktion sozialer Sachverhalte abzielt, wurde sich im Rahmen der Experteninterviews für ein Leitfadeninterview entschieden, da so die teils unterschiedlichen und lose miteinander verbundenen Aspekte und Antwortrichtungen der einzelnen Interviews am besten erfasst werden können (Gläser & Laudel, 2014, S. 43). Im Rahmen der vorgenommenen qualitativen Befragungen wurden drei persönlich-mündliche Hausinterviews sowie ein telefonisch-fernmündliches Interview durchgeführt. Die persönlich-mündlichen Hausinterviews werden in der Regel von einem Interviewer mit einem Gesprächspartner „face-to-face“ an einem verabredeten Ort, in diesem Fall dem Arbeitsplatz der Befragten, durchgeführt (Scholl, 2003, S. 31). Bei der Auswahl der Interviewpartner wurden die Befragten nicht zufällig ausgewählt, sondern aufgrund ihrer zuvor recherchierten Expertise und ihrer Profession ausgewählt, da die Datenschutz- und Online Marketing Thematik des Fragebogens ein umfangreiches Wissen auf diesen Gebieten voraussetzt. Der Autor dieser Arbeit bringt, durch eigene Recherche in diesen Bereichen sowie seine eigene Profession, die nötige Kompetenz mit, um im Rahmen der qualitativen Interviews komplexere und tiefere Informationen der einzelnen Interviewpartner zu erfragen, was einen Vorteil der gewählten Methodik ausmacht (Scholl, 2003, S. 40). Die fernmündliche Befragung ist zwar als weniger persönlich anzusehen als ein face-to-face Interview (Scholl, 2003, S. 41), musste bei einem Befragten jedoch durch die geographische Entfernung und damit verbundene Nichtumsetzbarkeit eines persönlich-mündlichen Hausinterviews durchgeführt werden. Wie bei den persönlich-mündlichen Interviews kann bei einem telefonischen Interview eine sehr hohe Befragungsqualität erzielt werden, die noch konzentrierter und kontrollierter ablaufen kann, da das Verhalten auf die akustische Dimension reduziert und weniger exponiert ist (Scholl, 2003, S. 44 zit. n. Fowler 1988; zit n. Fuchs 1994). Nachteilig kann hierbei sein, dass ein telefonisches Interview unpersönlicher und unverbindlicher ist als ein face-to-face Interview und die Interviewdauer in der Regel kürzer ist (Scholl, 2003, S. 45). Letztere Charakteristika konnten jedoch nicht beobachtet werden, da das telefonische Interview die vorgesehene Dauer von 30 Minuten überschritt und sehr tiefe Erkenntnisse zu Tage gefördert werden konnten.

Im Rahmen der persönlich-mündlichen und der fernmündlichen Befragung wurde sich für das Leitfaden- und Experteninterview entschieden. Hierbei strukturiert der Interviewer mit spezifischen Fragen anhand eines Interviewleitfadens das Gespräch und gibt den Befragten die Möglichkeit frei zu antworten, kann hierbei durch vertiefende Fragen, tiefere Erkenntnisse hervorbringen (Scholl, 2003, S. 66). Im Rahmen der hier durchgeführten Experteninterviews wurden zehn Fragen konzipiert, die sich auf die drei Kernbereiche Datenschutz, Auswirkungen von Datenschutz auf wirtschaftliche Prozesse und

die Nutzerperspektive beziehen. Werden mehrere Fragen bereits durch eine Antwort eines Interviewpartners beantwortet, so können einzelne Fragen des Interviewleitfadens ausgelassen werden (Scholl, 2003, S. 66). Da das Wissen von Experten in der Regel über vorformulierte Antwortmöglichkeiten hinausreicht, wurde auf solche verzichtet, beziehungsweise die Fragen so formuliert, dass sie wertfrei sind und keine Richtung vorgegeben wird (Scholl, 2003, S. 67). „Das Ziel des Experteninterviews besteht also allgemein in der Generierung bereichsspezifischer und objektbezogener Aussagen (Scholl, 2003, S. 67).“ Allen Interviewpartnern wurden sogenannte Schlüsselfragen im selben Wortlaut gestellt, um eine valide Beantwortung der Forschungsfragen dieser Arbeit zur generieren. Diese wurden durch Einleitungsfragen, Folgefragen, Nachhaken, Spezifizierunsfragen, Strukturierungsfragen und Interpretationsfragen ergänzt, um die teils unterschiedlichen Expertenfelder der Befragten zu nutzen, um unterschiedliche Perspektiven auf die Forschungsfrage zu generieren (Scholl, 2003, S. 68 f.). Alle Interviews wurden mit Hilfe technischer Endgeräte aufgenommen und in Transkripten protokolliert. Die sich im Anhang befindenden Transkripte werden Anhand einer qualitativen Inhaltsanalyse ausgewertet.

7.2.1 Auswahl der Experten

Bei der Auswahl der Experten gab es mehrere Voraussetzungen, die die Kandidaten zu erfüllen haben. Zum einen müssen die Experten in ihrer Profession mit dem Thema Datenschutz vertraut sein, zum anderen direkt an Prozessen mitwirken oder mitgewirkt haben, die sich mit der Umsetzung oder Interpretation der DSGVO befassen. Weiterhin sollte ein tiefgehendes Verständnis von Online Marketing Prozessen gegeben sein, um datenschutzrechtliche Vorgaben mit gängigen Praktiken von digitalen Geschäftsmodellen in Verbindung bringen zu können. Letztendlich wurden vier Experten ausgewählt, die sich in unterschiedlicher Weise mit der DSGVO und Datenschutz konfrontiert sehen. Zum einen wurde mit Ilka Voss eine Expertin auf dem Gebiet Real Time Advertising ausgewählt, die nebenbei eine Arbeitsgruppe im Online Marketing bei der OTTO GmbH & Co. KG leitet, die sich mit der Umsetzung der DSGVO und der ePVO auseinandersetzt. Als weitere Expertin wurde sich für Birgit Weyring entschieden, die als Datenschutz-Koordinatorin im Online Marketing der OTTO GmbH & Co. KG die Umstellung aller Bereiche des Online Marketings auf die DSGVO koordiniert. Mit dem Digitalisierungsberater und stellvertretenden Vorsitzenden der D21 Initiative e.V., konnte ein zertifizierter Datenschutzbeauftragter nach DSGVO interviewt werden, der als Wirtschaftsjurist Unternehmen in Datenschutzfragen berät und somit ein tiefes Rechtsverständnis einbringen kann. Letztlich wurde mit Andreas Sierts als Senior Director AI & Analytics von Adform, einer Advertising Technology Plattform, ein Fachmann aus dem

technischen Bereich des Online Werbemarktes interviewt, der die Umsetzung der DSGVO in einem Bereich betreut, der für Nutzer in der Regel verborgen bleibt, aber sehr stark auf datenbasierter Aussteuerung basiert.

7.2.2 Qualitative Inhaltsanalyse

Die in der qualitativen Erhebungsmethode generierten Rohdaten, in diesem Fall Transkripte der Leitfadeninterviews, müssen anhand einer qualitativen Auswertungsmethode auf relevante Information untersucht und anschließend interpretiert werden (Gläser & Laudel, 2014, S. 43). Hierbei wurde sich für die qualitative Inhaltsanalyse entschieden, bei der in einem systematischen Verfahren, relevante Informationen der Transkripte verschiedenen Kategorien zuzuordnen sind, bevor sie weiterverarbeitet werden (Gläser & Laudel, 2014, S. 46). Die hier vorgenommene Auswertungsmethode weicht in diesem Fall leicht von der qualitativen Inhaltsanalyse nach Mayring ab, da zwar auf ein Kategorisierungssystem zurückgegriffen wird, dieses aber entgegen Mayring weder geschlossen noch standardisiert ist, um dynamischer auf unvorhergesehene Informationen zu reagieren und diese auch dann in die Interpretation einfließen zu lassen, wenn diese nicht einer einzigen Analysekategorie zuzuordnen sind (Gläser & Laudel, 2014, S. 199). Es sollen demnach Informationen extrahiert werden und nicht Häufigkeiten, wie in der Mayringschen Inhaltsanalyse. Der Kern dieses Verfahrens bildet die Extraktion der relevanten Informationen aus den jeweiligen Transkripten, die den festgelegten Kategorien, also Untersuchungsvariablen oder Hypothesen, zugeordnet werden (Gläser & Laudel, 2014, S. 201). Da im Rahmen des Leitfadeninterviews allen Befragten dieselben Fragen gestellt wurden, können diese als Kategorien für die systematische Auswertung übernommen werden. Es werden keine deduktiv abgeleiteten Kategorien verwendet, sondern den Leitfragen entsprechende Themenbereiche. Die extrahierten Rohdaten werden daraufhin den festgelegten Kategorien und abgeleiteten Hypothesen zugeordnet und mit Quellenangaben versehen aufgeführt, nachdem die Texte systematisch nach relevanten Informationen durchgegangen wurden (Gläser & Laudel, 2014, S. 204). Die Transkripte der Experteninterviews befinden sich im Anhang und werden nach folgendem System zitiert: E1 = Experteninterview 1, XX = Namenskürzel, 33-36 = zitierte Zeilen.

7.2.3 Forschungshypothesen

Die festgelegten Kategorien entsprechen den Themen, die im Rahmen der Leitfadeninterviews abgefragt wurden. Aus diese Themenbereichen wurden sechs Hypothesen abgeleitet, die im Rahmen der Inhaltsanalyse verifiziert oder falsifiziert und anhand der

verschiedenen Expertenstimmen diskutiert werden sollen. Folgende Hypothesen wurden aus den in dieser Arbeit diskutierten Themenbereichen abgeleitet:

Experteninterview-Kategorie 1: Relevanz der DSGVO	**Hypothese 1:** Eine neue Gesetzgebung hinsichtlich Datenschutz ist notwendig.
Experteninterview-Kategorie 2: Auswirkungen der DSGVO auf das Online Marketing	**Hypothese 2:** Die DSGVO hat einschneidende Auswirkungen auf Online Marketing Prozesse.
Experteninterview-Kategorie 3: Auswirkungen auf die Marktmacht von Google und Facebook	**Hypothese 3:** Die DSGVO wirkt sich positiv auf die Marktmacht der großen Unternehmen auf dem Werbemarkt wie Google oder Facebook aus.
Experteninterview-Kategorie 4: Auswirkungen auf die Marktbemühungen der Unternehmen	**Hypothese 4:** Die DSGVO bringt Unternehmen dazu ihre Marktbemühungen hinsichtlich Datenschutz zu überdenken.
Experteninterview-Kategorie 5: Auswirkungen auf das Nutzerverhalten	**Hypothese 5:** Nutzer werden in Zukunft stärker von ihren Betroffenenrechten Gebrauch machen und vermehrt das Opt-In verweigern, auch wenn die User Experience darunter leidet.
Experteninterview-Kategorie 6: Informationelle Selbstbestimmung der Nutzer	**Hypothese 6:** Durch die DSGVO wird der Nutzer zukünftig selbstbestimmter im Netz agieren.

7.3 Gruppendiskussion Nutzerverhalten

Als zweite empirische Methode wurde eine Gruppendiskussion durchgeführt. Nachdem die DSGVO in ihren Auswirkungen von Experten bewertet wurde, soll nun ein Fokus auf das Nutzerverhalten gelegt werden. In einer sogenannten Fokusgruppe sollen Kommunikationsprozesse initiiert werden, die einem alltäglichen interaktiven Gespräch zwischen den Teilnehmern ähneln soll (Vogl, 2014, S. 581). Da die Teilnehmer eine Einschätzung ihres eigenen Nutzerverhaltens und ihres Umgangs mit ihren Daten und ihrer Privatsphäre abgeben sollen, ist es vorteilhaft, einen natürlichen diskursiven Austausch zu fördern, da die Teilnehmer hier eher als in einem persönlichen Face-to-Face Interview dazu neigen, ihre ehrliche Meinung einzubringen (ebd.). Ziel ist es durch die entstehende Gruppendynamik tieferliegende Einstellungen zu erforschen und durch den Charakter einer öffentlichen Diskussion, eine Art „öffentliche Meinung“ zu erfassen (Scholl, 2003,

S. 117). Derart kollektive Orientierungen im Entstehungsprozess zu erfassen ist der große Vorteil einer Gruppendiskussion, da sich Teilnehmer einer Befragung oft erst im Gespräch gezwungen sehen ihre Meinung zu äußern und ihren Standpunkt klar zu vermitteln (Vogl, 2014, S. 582). Nachteilig kann sein, dass sich ein Meinungsführer hervortun kann, so dass extreme Gruppenmeinungen entstehen oder eine hohe Schweigerquote eintritt. Die Gruppendiskussion wird anhand eines Leitfadens initiiert, der aus rein offenen Fragen besteht, die nur relevante Sachverhalte antizipieren dürfen, denn die Diskussion darf sich nicht zu einer Gruppenbefragung entwickeln (Scholl, 2003, S. 118). Dennoch ist es möglich einzelne Sachverhalte abzufragen, um Gesprächsdynamiken anzuregen und die Gruppe thematisch zu steuern.

7.3.1 Planung, Leitfaden und Durchführung

Ziel der Gruppendiskussion ist es herauszufinden, wie die Teilnehmer ihre Privatsphärebedenken äußern, wie sie mit ihren Daten umgehen und zu welchen Handlungen oder Abstrichen aufgrund des Datenschutzes sie bereit wären. Da kein Experiment sondern eine explorative Gruppendiskussion durchgeführt wird, beschränkt sich das Forschungsdesign auf eine Gruppe mit sechs Teilnehmern. Da eine gewisse digitale Affinität vorgesehen ist, um die Thematik des Diskurses zu durchdringen und beurteilen zu können, wurde sich für eine Realgruppe und nicht eine künstliche Gruppe entschieden, da eine ähnliche demographische Grundlage der Teilnehmer in diesem Feld zu einem authentischeren Gespräch führen soll (Scholl, 2003, S. 119). Die Gruppe setzt sich sowohl aus männlichen als auch aus weiblichen Teilnehmern zusammen, die in der folgenden Ergebnisauswertung jedoch im Sinne des generischen Maskulinums als Teilnehmer bezeichnet werden. Den Teilnehmern werden Fragen zu ihrem Nutzungsverhalten und ihren Privatsphärebedenken gestellt, um theoretisch untersuchte Phänomene wie das Privacy Paradoxon zu prüfen und zu evaluieren welche Bedürfnisse der Nutzer bezüglich seiner Daten und Datenschutz hat. Hierfür dient ein Leitfaden, der aber nur aus offenen Fragen besteht und nur den Rahmen für die Diskussion vorgibt, auf die im Falle zu großer Konformität von Seiten des Moderators reagiert werden kann, um eine kontroversere Diskussion anzuregen (Vogl, 2014, S. 583). Der Moderator kann während der Diskussion die Techniken der Paraphrasierung, Entschleunigung, Projektion, Visualisierung, Konfrontation oder Provokation anwenden, um Details, Vertiefungen und Emotionen aufzudecken (Vogl, 2014, S. 585). Die Fokusgruppe soll hierbei durchgehend in einer Diskussionsdynamik bleiben, weswegen nur dann eingegriffen wird, wenn die Thematik abschweift oder aus Gründen des Zeitmanagements einzelne Themenbereiche angesprochen werden müssen.

Die gesamte Diskussion wird aufgenommen und transkribiert, um anschließend eine qualitative Inhaltsanalyse durchzuführen. Hierbei werden Inhalte, Auffälligkeiten und Besonderheiten gesammelt und miteinander in Beziehung gesetzt, um ein zentriertes Gesamtbild der Fokusgruppe zu skizzieren (Scholl, 2003, S. 122). Konformitäten und Nonkonformitäten werden hierbei ebenfalls identifiziert. Die gesammelten Inhalte werden nicht einzelnen Kategorien zugeordnet, wie bei den Experteninterviews, sondern als facettenreiches Gesamtbild erfasst. Die Aussagen der Teilnehmer, dienen nicht zur Falsifizierung oder Verifizierung der Hypothesen dieser Arbeit, sondern sollen Einblick in die kognitiven Prozesse der Nutzer geben, um sie abschließend auf die Hypothesenprüfung der Expertenbefragungen beziehen zu können. Das Transkript der Gruppendiskussion befindet sich im Anhang und wird nach folgendem System zitiert: T1 = Teilnehmer 1, 33-36 = zitierte Zeilen. Über den Namen sowie weitere personenbezogenen Daten der Teilnehmer der Gruppendiskussion herrscht Diskretion.

7.3.2 Diskussionsleitfaden

Der Diskussionsleitfaden beinhaltet verschiedene offene Fragen zum Nutzerverhalten, den Privatsphärebedenken der Nutzer, zu ihren Datenschutzvorkehrungen und zu ihren Bedürfnissen in Bezug auf Datenschutz und User Experience. Folgende Fragen sollen den zentralen Diskussionsrahmen vorgeben.

1) Welche digitalen Dienste nutzt ihr regelmäßig und warum?
2) Habt ihr Privatsphärebedenken bei der Nutzung dieser Dienste, wenn ja welche?
3) Ist euch Datenschutz wichtig?
4) Willigt ihr regelmäßig bei Consent-Verfahren ein, ohne Datenschutzrichtlinien oder mitgelieferte Informationen über Cookies und Tracking gelesen zu haben?
5) Würdet ihr bei Unternehmen eure personenbezogenen Daten anfragen, löschen oder berichtigen?
6) Würdet ihr für Datenschutz zahlen oder Abstriche in der User Experience machen?

Sollten diese Fragen nicht die gewünschten Diskussionsdynamiken initiieren, wird sich der Moderator mit punktuellen Erläuterungen in die Diskussion einbringen oder einzelne Teilnehmer dazu motivieren, ihre Ausführungen zu vertiefen. Der Aufbau der Fragen wurde bewusst so gewählt, damit die Nutzer nicht wissen, dass sie zu ihren Schutzvorkehrungen und ihrem Privatsphärebedenken befragt werden, bevor sie ihr eigenes Nutzerverhalten skizzieren.

8 Vorstellung der Ergebnisse

Im folgenden Kapitel werden die Ergebnisse der qualitativen Inhaltsanalyse der Experteninterviews und der Gruppendiskussion vorgestellt, die abgeleiteten Hypothesen geprüft und diskutiert. Die Ergebnisse der Expertenbefragung sollen zum einen die theoretische Diskussion dieser Arbeit mit marktinternen und fachbezogenen Stimmen ergänzen und zum anderen einen Ausblick für die Branche skizzieren, um abschließend ein Fazit zur DSGVO ziehen und eine Zukunftsprognose für den Datenschutz und das Nutzerverhalten geben zu können. Die Ergebnisse der Gruppendiskussion sollen Aufschluss über das Nutzerverhalten, etwaige Privatsphärebedenken sowie Phänomene wie da Privacy Paradoxon geben und ebenfalls als Grundlage für Handlungsempfehlungen und eine Zukunftsprognose der Nutzerrolle dienen.

8.1 Experteninterview-Kategorie 1: Relevanz der DSGVO

Hypothese 1: Eine neue Gesetzgebung hinsichtlich Datenschutz ist notwendig.

Alle Interviewpartner halten die Einführung einer neuen, harmonisierten Gesetzgebung hinsichtlich Datenschutz auf europäischer Ebene für notwendig. Grund hierfür sind zum einen die veralteten vorangegangenen Gesetzgebungen sowie die digitale Weiterentwicklung der Welt (E1, IV, 3-5). Die DSGVO ist also zeitlich und durch den technologischen Fortschritt bedingt sehr relevant, hat dem Datenschutzbeauftragten Björn Stecher zufolge aber dennoch Bestandteile, die keine Antworten auf gewisse Zukunftsszenarien bieten (E3, BS, 41-43). Ebenfalls kann der DSGVO attestiert werden, dass sie zuvor ungenaue Rechtsgrundlagen präzisiert und auf europäischer Ebene harmonisiert (E4, AS, 35-41), sowie Begriffe wie den Personenbezug präzisiert und Grundlagen für Transparenz gegenüber dem Nutzer schafft, was besonders für Technologie-Unternehmen aus der Online-Werbebranche wichtig ist, da diese einen gewissen Vertrauensvorschuss der User brauchen (E4, AS, 44-46). Ebenfalls können marktineffiziente Sonderlösungen, wie die in Deutschland gängige Einwilligungsverweigerung durch ein Opt-Out, nach TMG nun harmonisiert vermieden werden (E2, BW, 17-34). Für den Anwendungsbereich der DSGVO wird der Personenbezug nochmals präzisiert, jedoch wird die Frage aufgeworfen, ob es hier eine Trennung perspektivisch überhaupt noch geben darf, da wie in Kapitel 3.1 dargestellt, bei den meisten Daten ein Personenbezug immer irgendwie hergestellt werden kann (E3, BS, 45-47). Stecher stellt hier die These auf, dass Datenschutz in gewisse Datenkategorien aufgebrochen werden müsste, die verschiedener Datensicherheitsniveaus bedürfen und man dementsprechend jeweils andere Rechtskonsequenzen daran anschließen könnte (E3, BS, 49-61). Dieses Kaskadenmodell hätte demnach zur Folge, dass die Nutzer in ihrem subjektiven Datenschutz besser abgeholt werden würden (E3, BS, 62-63). Ebenfalls wird angemerkt, dass in der DSGVO neue

Instrumentarien zum Datenschutz fehlen, da die Komplexität und Multidimensionalität von Tracking-Verfahren und Datenverarbeitung mit nicht genügend Transparenz begegnet wird und man mit Einwilligungsverfahren zwar ein Instrument bereitstellt, dieses aber weiterhin die Hauptverantwortung auf die Nutzer abwälzt, die die Konsequenzen nicht kritisch reflektieren können (E3, BS, 71-89). Zusammenfassend attestieren alle Experten der DSGVO eine hohe Relevanz, sehen in der Ausführung aber viele offene Fragen und wünschen sich einen stärkeren Bezug auf einzelne Datenkategorien und Anwendungsbereiche.

8.2 Experteninterview-Kategorie 2: Auswirkungen der DSGVO auf das Online Marketing

Hypothese 2: Die DSGVO hat einschneidende Auswirkungen auf Online Marketing Prozesse.

Die Einschätzungen der Experten gehen zunächst dahin, dass die Auswirkungen der DSGVO Prozesse im Online Marketing nicht einschränken werden, jedoch zu einem deutlichen Mehraufwand führen (E1, IV, 37-38). Auch datenbasierte Aussteuerungen wie programmatischer Einkauf von Werbeplätzen wird nach wie vor möglich sein, es müssen nun aber technische und organisatorische Maßnahmen (TOMs) getroffen werden, um die gestärkten Betroffenenrechte im Zweifel bedienen zu können (E2, BW, 49-53). Ebenfalls wird durch die zuvor angesprochene normative Unschärfe eine gewisse Unsicherheitsphase in der Branche ausgelöst, die zur Folge hat, dass Unternehmen vorsichtiger in Bezug auf Maßnahmen und die Zusammenarbeit mit externen Marketingpartnern agieren könnten (E2, BW, 45-67). Ganz explizit hat die DSGVO hier zur Folge, dass Werbetreibende, Publisher oder AdTech Unternehmen ihre Vertragsverhältnisse mit ihren Partnern ergänzen müssen, da klar rechtlich geregelt sein muss, dass eine Einwilligung für das Setzen von Cookies eingeholt werden muss (E4, AS, 69-74). Dies ist darauf zurückzuführen das Cookies, Cookie-IDs und Online Identifier von Unternehmen konkret als personenbezogenes Datum behandelt werden müssen, also zustimmungspflichtig sind (E4, AS, 59-66). Dies bedeutet, dass auch Technologie Dienstleister wie DSPs, DMPs oder Adserver technische Maßnahmen treffen müssen, um die Betroffenenrechte bedienen zu können, Daten zu prozessieren und Einwilligungen einzuholen. Ebenfalls werden für das Targeting verwendete Verfahren, wie Profiling strenger behandelt, so dass ein Zusammenführen von Daten mit dem Zweck der Profilierung zumindest auskunftspflichtig ist (E3, BS, 100-105).

Die beschriebene normative Unschärfe gepaart mit den gestärkten Betroffenenrechten und den Cookie-Bannern führt dazu, dass Unternehmen im Online Marketing einen

Spagat zwischen vollständiger Information und einfachen Erklärungen zum Datenschutz leisten müssen, was bereits mehrere Zielkonflikte in sich birgt, da die Komplexität der Verfahren in einfachen Erklärungen schwer darstellbar ist (E3, BS, 112-119). Diesen Spagat sieht auch Andreas Sierts, der mit Adform Teil des IAB Consent Frameworks ist und Tools anbietet, mit denen sich Cookie Banner prominent und DSGVO konform auf der Website einbetten lassen (E4, AS, 92-102). Hinzu kommt die Unsicherheit, welche Erweiterungen bzw. Verschärfungen mit der ePrivacy-Verordnung geben wird. Auf Unternehmensseite ist man sich sicher, dass diese noch einmal ein verschärftes Opt-In nach sich ziehen wird und somit größere Auswirkungen auf das Online Marketing hat (E2, BW, 89-103). Die Experten rechnen jedoch nicht mehr dieses Jahr mit der ePVO und verweisen darauf, dass es wahrscheinlicher ist, dass sie 2019 (E4, AS, 122-124) im Herbst (E3, BS, 139-140) in Kraft tritt, nachdem sie eigentlich schon zum Start der DSGVO fertig sein sollte und im Idealfall in diese eingebettet werden müsste (E3, BS, 147-149). Interessant wird dann die Frage sein, wie etwaige Verschärfungen im Bereich der Einwilligung (Consent) umgesetzt werden, ob durch Consent-Frameworks von unabhängigen Drittanbietern oder ob die Browser die Hoheit über den Opt-In bekommen (E4, AS, 131-138).

8.3 Experteninterview-Kategorie 3: Auswirkungen auf die Marktmacht von Google und Facebook

Hypothese 3: Die DSGVO wirkt sich positiv auf die Marktmacht der großen Unternehmen auf dem Werbemarkt wie Google oder Facebook aus.

In diesem Punkt sind sich alle Experten einig, auch wenn sich die DSGVO finanziell negativ auf Google und Facebook auswirkt, werden diese Unternehmen diejenigen sein, die die neue Verordnung leichter umsetzen können (E3, BS, 156-157). Dies liegt zum einen an den notwendigen Realisierungselementen, die diese Unternehmen haben (E3, BS, 161-163, zum anderen an der Monopolstellung, die Google und Facebook beinahe besitzen (E1, IV, 55-58), da sie ein Produkt anbieten, auf das keiner verzichten kann oder mag. Hier attestieren die Experten Google und Facebook besonders darin einen Vorteil, dass sie es als Plattformen, die über ein Login der Nutzer laufen, leichter haben einen Opt-In zu generieren und diesen an ihre Datenschutzrichtlinien koppeln können (E1, IV, 58-61). Google und Facebook werden durch das Gesetz nicht bevorzugt, haben durch ihren Marktanteil und ihre starken Produkte in der Konsequenz einen Vorteil gegenüber kleineren Marktteilnehmern und mittelständischen Unternehmen, für die der organisatorische Aufwand viel größer ist (E2, BW, 174-179). Wie zuvor angesprochen könnten Browser-Voreinstellungen die Lösung für Consent-Verfahren sein. Da zum Beispiel der weit verbreitete Chrome Browser ein Produkt von Google ist und auch die

Facebook Applikationen ein geschlossenes Ökosystem bilden, könnten die marktdominanten Unternehmen starken Einfluss auf etwaige Verfahren ausüben (E2, BW, 213-219). Ein weiterer wichtiger Punkt, der Google und Facebook betrifft, ist der, wie Daten von Dritten verarbeitet werden. So verbietet Google seit der DSGVO Third-Party-Tracking auf YouTube, so dass keiner außer Google mehr die Performance von Kampagnen messen kann (E4, AS, 146-151). Auf der anderen Seite ist der Marktdruck auf die großen Unternehmen nicht zu unterschätzen. So hatte Google vor, ein eigenes Consent-Tool auf den Markt zu bringen, in dem die Nutzer ihre Präferenzen auswählen können, welchen Dienstleistern sie ein Opt-In geben und welchen nicht. Google erlaubte hier aus Gründen zu hoher Komplexität für den Nutzer jedoch nur 10 verschiedene Dienstleister, was den Todesstoß für viele Unternehmen und Start-Ups der Advertising Technology Branche bedeutet hätte. Auf Druck der Industrie nahm Google den Vorstoß wieder zurück und scheint sich am IAB Consent-Framework zu beteiligen (E4, AS, 156-167).

Auch der mediale und politische Druck der auf Facebook lastet, seitdem Cambridge Analytica an eine Vielzahl an Facebook-Nutzerdaten gelangen konnte, ist sehr groß, scheint jedoch nicht zur Folge zu haben, dass Facebook große Einschnitte zu erwarten hat. Zu komplex ist Facebook als Konzern und zu komplex die Algorithmen die verwendet werden, um datenschutzrechtlich gegen die Praktiken Facebooks vorzugehen und zu prüfen wie pesudonymisiert die Daten wirklich sind und welchen Aufwand es bedürfe, diese zu deanalysieren um einen Personenbezug herzustellen (E3, BS, 167-178). Zusammenfassend ist zu sagen, dass die DSGVO als Gesetz keine Bevormundung oder Benachteiligung der großen Marktteilnehmer darstellt, jedoch zu einer Stabilisierung der Marktmacht von Google und Facebook führen wird, da sie zum ersten leichter auf Datenschutzverschärfungen reagieren können, es zweitens leichter haben werden Einwilligungen einzuholen bzw. durch Logins bereits eingeholt haben und zum dritten an der Umsetzung von technischen Verfahren zum Datenschutz mitarbeiten können.

8.4 Experteninterview-Kategorie 4: Auswirkungen auf die Marktbemühungen der Unternehmen

Hypothese 4: Die DSGVO bringt Unternehmen dazu ihre Marktbemühungen hinsichtlich Datenschutz zu überdenken.

Die Experten sehen in der DSGVO einen Anstoß dafür, dass Unternehmen ihre Praktiken überdenken und zukünftig sensibler mit personenbezogenen Daten umgehen werden (E4, AS, 209-210). Die Datenschutz- und Real Time Advertising Expertin bei OTTO, Ilka Voss, sieht in der gesteigerten Relevanz von Datenschutz sogar die Chance für Unternehmen, sich am Markt mit einem transparenten und sicheren Umgang mit Daten

zu positionieren (E1, IV, 99-102). Von Nöten wird jedoch auch sein, dass Unternehmen noch genauer überprüfen, mit wem sie zusammenarbeiten und wie leichtfertig sie Kundendaten für Marketingzwecke an Drittanbieter weitergeben und so ein Reputationsrisiko eingehen (E4, AS, 196-200). Um diesem Verhältnis gerecht zu werden, schlägt der Datenschutzexperte Björn Stecher einen Daten-Ethik-Code in Form einer Corporate Digital Responsibility (CDR) vor, die sich jedes Unternehmen auferlegt und nach der sie die eigene Verwendung der Daten einer ethischen Grundprüfung unterzieht (E3, BS, 198-211). Eine im Aktien- und GmbH-Gesetz festgehaltene Pflicht zu einer CDR, würde den internen Druck erhöhen, Datenschutzverletzungen sanktionierbar machen und einen größeren Einfluss haben, als strengere Gesetze (E3, BS, 212-221).

8.5 Experteninterview-Kategorie 5: Auswirkungen auf das Nutzerverhalten

Hypothese 5: Nutzer werden in Zukunft stärker von ihren Betroffenenrechten Gebrauch machen und vermehrt das Opt-In verweigern, auch wenn die User Experience darunter leidet.

In der Frage ob mehr Nutzer in Zukunft auf Websites den Opt-In verweigern werden, kommen die Experten zu einer beinahe einstimmigen Beurteilung. Zwar werden durch die steigende Sensibilisierung auf Grund der DSGVO mehr Nutzer zunächst das Opt-In verweigern, jedoch wird sich mit der Zeit keine wesentliche Steigerung einstellen (E3, BS, 225-229). Dies ist darauf zurückzuführen, dass Unternehmen es zum einen schaffen werden, ausreichend Bequemlichkeit für den Nutzer anubieten, zum anderen interessiert es die meisten Nutzer nicht, was im Hintergrund mit ihren Daten passiert, wenn das Produkt gut genug oder der Nutzen der Anwendung groß genug ist, äußert die DSGVO Spezialistin Birgit Weyring (E2, BW, 255-257). Hier könnten auch Incentivierungen eine Rolle spielen, also gewisse Vorteile bei der Nutzung der Seite, Rabatte oder besondere Angebote (E1, IV, 131-134). Ähnlich wie bei dem Opt-In gehen die Erwartungen bei der Ausübung von Betroffenenrechten dahin, dass aus Gründen der Bequemlichkeit nur eine Minderheit der Nutzer von seinen neuerdings gestärkten Rechten Gebrauch machen wird (E2, BW, 290-291). Wie beim Opt-In ist zwar zu erwarten, dass es einen kleinen Peak geben wird dieses Jahr (E3, BS, 247-249), dass dies aber eher Leute mit einem besonderen Interesse oder einer professionellen Beziehung zum Thema Datenschutz machen werden (E4, AS, 216-220). Grund hierfür kann zum einen die Trägheit der Nutzer sein (E1, IV, 140-141), zum anderen erfordert es eine gewisse Kompetenz einschätzen zu können, ob man überhaupt Betroffener ist und welche Daten wo hinterlegt sind (E3, BS, 241-243). So wissen viele Nutzer ebenfalls nicht welche Daten und auf welchem Weg sie Daten erfragen können. Besonders dann, wenn Daten pseudonymisiert

verarbeitet werden, müsste der Nutzer beispielsweise seine Cookie-ID mitschicken, da Cookies nicht in Verbindung mit einem Namen oder einer E-Mail-Adresse gespeichert werden (E4, AS, 223-227). Das übersteigt die Kompetenz der meisten Nutzer. Laut Andreas Sierts, bietet Adform eine Privacy Center auf ihrer Homepage an, wo der Nutzer über seinen Browser, mit Hilfe seiner Browser-ID, seine Daten beantragen und löschen lassen kann. Hinzu kommt, dass Datenschutzrichtlinien sich jetzt noch transparenter, also noch umfangreicher gestalten werden, was auch nicht im Sinne der Nutzer und im Sinne des Gesetzes ist (E2, BW, 261-263). Zusammenfassend werden die gestärkten Betroffenenrechte trotz zahlreicher Diskrepanzen als positiv aufgefasst, da sie in der Theorie wichtig für die informationelle Selbstbestimmung der Nutzer sind und man nun besser seine Spuren bei einem Unternehmen beseitigen kann (E2, BW, 311-316). Es stellt sich aber die Frage, ob dies den immensen Aufwand, der auf die Unternehmen zukommt, rechtfertigt (E1, IV, 150-151). Außerdem stellt sich die Frage, ob die User Experience unter der Zunahme von Consent-Verfahren leiden wird und ob der Datenschutz den Nutzern der Verlust eines flüssigen Erlebnisses wert ist. Ein Wegfallen von personalisierten Inhalten aufgrund vorgenommener Privatsphäre Präferenzen würde für viele Nutzer ein Negativerlebnis darstellen und sie dazu motivieren einem Unternehmen doch die Einwilligung zur Datenverarbeitung zu erteilen (E1, IV, 210-223). Einige EU-Länder interpretieren die DSGVO weiterhin so, dass im Weitersurfen die Einwilligung besteht, es also einen Hinweis auf Cookie-Dropping gibt, die User Experience aber nicht weiter gestört wird, was auch im Sinne des Users sein dürfte (E4, AS, 252). Alternativ könnte es sich rechtlich so herausstellen, dass ohne Einwilligung Seiten nicht mehr aufrufbar wären oder der Nutzer bei jedem Websiteaufruf für jedes Tracking-Verfahren eine Einwilligung geben muss (E4, AS, 242-256). Es wird bei Consent-Verfahren im Zweifel immer auf die Frage hinauslaufen, ob eine Einwilligung wirklich als selbstbestimmte Handlung eines Nutzers im Netz aufgefasst werden kann.

8.6 Experteninterview-Kategorie 6: Informationelle Selbstbestimmung der Nutzer

Hypothese 6: Durch die DSGVO wird der Nutzer zukünftig selbstbestimmter im Netz agieren.

Mit gestärkten Betroffenenrechten, Verpflichtungen zum Einholen von Opt-Ins beim Setzen von Cookies oder weiteren Tracking-Verfahren sowie der Verpflichtung zur technischen Ausgestaltung im Sinne von Privacy by Default und Privacy by Design, versucht die europäische Union die Nutzerrechte zu stärken und die informationelle Selbstbestimmung zu steigern. Die Experten beurteilen diese Zielsetzung und ihre Umsetzung

unterschiedlich, äußern jedoch auch Vorschläge wie Nutzer wirklich selbstbestimmt agieren könnten. Zum einen konnten Nutzer bereits vor der DSGVO ihre Cookies löschen und somit ihre Datenströme kappen, es haben nur sehr wenige getan (E2, BW, 271-275), zum anderen kann Selbstbestimmtheit auch so interpretiert werden, dass man die Entscheidung bewusst trifft eine Website oder ein Programm zu nutzen, gerade wenn man dafür mit seinen Daten bezahlt. Auch bedeutet ein Opt-In nicht gleich, dass Nutzer dadurch selbstbestimmter sind, mit einer Einwilligung, die nicht immer auf einer ernsthaften Abwägung basiert, geben sie schnell ihre Selbstbestimmtheit an die Konzerne ab (E2, BW, 169-171). Des Weiteren wird die ständige Abfrage eines Opt-Ins die User Experience negativ beeinflussen, da sie zum einen ein flüssiges Erlebnis stört und zum anderen Seiten bei einem verweigerten Opt-In gar nicht oder nicht personalisiert dargestellt werden (E1, IV, 210-226).

Einig sind sich die Experten, dass Privacy by Design and Default nicht zur Steigerung der Selbstbestimmung beiträgt. Es klingt zwar nach einem guten Ansatz, jedoch ist es fragwürdig, die Grundeinstellung zwecks der Privatsphäre eines Nutzer von den Unternehmen vornehmen zu lassen, die einen Browser oder eine App bereitstellen (E2, BW, 216-222). So würde eine Privacy by Default Einstellung in einem Browser bedeuten, dass der Nutzer selbstständig eine Rückeinstellung vornehmen müsste, wenn er Personalisierung auf Websites oder Vorteil durch Trackingverfahren wünscht (E1, IV, 156-162). Demnach würde der Nutzer vielmehr in seinem selbstbestimmten Verhalten beschnitten werden, da die Rückeinstellung ein Verständnis der Komplexität der Technik bedarf und die Browseranbieter die Weichen so stellen können, dass der Nutzer sich nach ihren Vorstellungen orientiert, im Zweifel bei der Benutzung eine Chrome Browsers von Google also die Voreinstellungen so interpretiert, nur noch Google seine Daten zur Verfügung zu stellen (E1, IV, 164-173). So kann Privacy by Design and Default im schlimmsten Fall bedeuten, dass keine Login-Daten mehr gespeichert werden, da Cookies nicht mehr gesetzt werden können (E2, BW, 227-230), oder das ganze Geschäftsmodelle nicht mehr funktionieren, da das ganze Thema besonders dann absurd wird, wenn man Smart Technology in Autos, Smart Home und generell an das Internet of Things denkt, also an Produkte die ihren hohen Nutzwert auf einer automatisierten Datenverarbeitung aufbauen (E3, BS, 250-255). In dem Ausbau von Datensouveränität und digitaler Kompetenz durch Schulen und Unternehmen sieht der Datenschutzexperte Björn Stecher ein wichtiges Mittel, damit Nutzer wirklich selbstbestimmt agieren können, Gesetze allein reichen nicht (E3, BS, 279-281). Weiterhin schlägt er eine technische Lösung vor, wie Nutzer komplett selbstbestimmt Kontrolle über ihre Daten gewinnen können und dadurch sogar Kompetenz erlangen können. Dies wäre möglich durch ein Datenportemonnaie, welches der Nutzer selber pflegt, also nur die präferierten Daten

preisgibt, und auf das Unternehmen komplett transparent über eine Schnittstelle zugreifen, wenn sie Daten benötigen (E3, BS, 305-319). Zusammenfassend wird sich der Nutzer durch die DSGVO nicht wirklich selbstbestimmter bewegen, viel entscheidender könnten Maßnahmen sein, die direkten Einfluss auf unternehmerische Praktiken haben und die Unternehmen zu Einhaltung von ethischen Grundsätzen und eigener Proaktivität zum Datenschutz motivieren.

8.7 Ergebnisse der Gruppendiskussion

Im Rahmen der Gruppendiskussion wurde das Nutzerverhalten der Teilnehmer und die damit einhergehenden Privatsphärebedenken untersucht. Als Grundlage zur Bewertung der geäußerten Bedenken bezüglich der Privatsphäre, wurde zunächst abgefragt, welche digitalen Dienste die Teilnehmer regelmäßig nutzen, um herauszufinden wo die Probanden ihre Datenspuren hinterlassen. Es wurde vorher nicht erwähnt, dass sie im Laufe der Diskussion ihre Privatsphärebedenken äußern sollen, damit sie nicht datenbezogenes Nutzerverhalten verschweigen und möglicherweise sogar eigenständig auf das Thema Datenschutz zu sprechen kommen. Ziel der Fragestellung war es, bei den Nutzern die kognitiven Phänomene des Privacy Calculus und Privacy Paradoxons zu identifizieren. Alle Beteiligten gaben einstimmig an regelmäßig den zu Facebook zugehörigen Messenger-Dienst WhatsApp zu nutzen und einen aktiven Facebook Account zu besitzen (T1-6, 8-32). Überdies hinaus nutzen vier von sechs Teilnehmern das von Facebook übernommene soziale Netzwerk Instagram (T1, T3, T4, T6, 14-18). Weiterhin nutzen alle Teilnehmer der Gruppendiskussion regelmäßig die Google Suchmaschine, Google Maps und besitzen einen Google Mail Account, privat und/oder beruflich (T1-6, 50-78). Überdies hinaus kommen die Teilnehmer regelmäßig mit weiteren Google Produkten, wie Drive, Calendar, Hangout, Chrome, Books und Scholar in Berührung (T1-6, 52-76). Innerhalb der Diskussion kam das Thema Mobilität auf, das mehrstimmig mit Google Maps und den Anbindungen anderer Mobilitäts-Applikationen an Googles Karten- und Navigationssystem in Verbindung gebracht wurde (41-48). Die einzigen Dienste, die nicht Teil der Ökosysteme von Facebook und Google sind und erwähnt wurden, sind der E-Mail-Provider Yahoo (T2, 13) und das professionelle Organisations-Tool Asana (T5, 30-32). Auf die vertiefende Frage hin, warum die Teilnehmer hauptsächlich Dienste von Facebook und Google nutzen, entstand eine interessante Diskussion, die verschiedene Haltungen gegenüber Facebook und Google zu Tage förderte. Besonders Google besticht hier durch verschiedene Vorteile, die Nutzer mit dem Tech-Giganten in Verbindung bringen. So ist die Omnipräsenz und das breite Produktportfolio einer der Hauptgründe für die Nutzung dieser Dienste, da man alle wichtigen Dienste zentriert unter einem Benutzerkonto führt (T6, 58-61). Ebenfalls als großer Vorteil wird

die Vernetzung und die Zusammenarbeit mit den eigenen Kontakten hervorgehoben, die besonders im Berufsleben sehr hilfreich sind (T3, 62-64). Mehrere Teilnehmer merkten an, dass ihnen gar kein Konkurrent für Google einfallen würde, was zu kollektiver Bestätigung aller Diskussionsteilnehmer führte (T1-T6, 65-71).

Ein Teilnehmer stellte die These auf, dass die Konkurrenzlosigkeit von Facebook deutlich eher anzufechten sei, da man den Messenger Dienst nicht nutzen müsste, da man ja WhatsApp als Alternative besäße (T1, 79-80). Dem entgegnete ein anderer Teilnehmer, dass WhatsApp ja zu Facebook gehöre und, dass man aus Gründen der Datensicherheit zu dem Messenger-Dienst Telegram wechseln müsste (T2, 82-83). Diese Feststellung führte dazu, dass die Diskussion sich selbstständig in die Datenschutzthematik bewegte. Der Teilnehmer führte weiter aus, dass er ein besonderes Vertrauen in die Professionalität des Datenschutzes bei Google legen würde, da sie sehr viel Arbeitskraft und Fokus auf Datensicherheit legen würden und, dass persönliche Daten nicht an Externe weiterverkauft würden, auch wenn Google als Werbenetzwerk agiert (T2, 83-92). Bei Facebook hingegen würden die eigenen Daten frei an Dritte verkauft werden (T2, 93-94). Eine Ansicht, die die sich in Frage stellen lässt. Zweckentfremdete Nutzerprofile wie im Fall von Cambridge Analytica sind auf ein Datenleck und nicht auf gängige Geschäftspraktiken von Facebook zurückzuführen. Ein anderer Teilnehmer bringt diese Sicht auf Facebook direkt mit der schlechten PR der letzten Jahre für Facebook in Verbindung (T6, 95-96).

Bei der Nutzung von Facebook zeigen sich große Unterschiede zwischen den Privatsphärebedenken der Teilnehmer, bzw. ihrem Umgang mit ihrer Privatsphäre. Zwei Teilnehmer gaben an, dass sie ihr Vertrauen in Datensicherheit bei Facebook aufgegeben hätten und ihren Facebook Account inflationär für den Login bei allen möglichen Applikationen und Websites verwenden, weil es die einfachste Lösung ist (T3, T4, 97-128). Diese Sichtweise bestätigt das in der Theorie hergeleitete Privacy Paradoxon, also hohe Privatsphärebedenken zu äußern, sich aber nicht dementsprechend zu schützen. Andere Teilnehmer bewerteten ihr Verhältnis zu Facebook ganz anders und hoben hervor, dass gerade der Facebook Account immens viele persönliche Informationen sowie Informationen über die Kontakte und Freunde und besuchte Websites beinhalte, und deswegen besonders schützenswert sei (T1, T2, T5). Die Privatsphärebedenken äußern sich bei Facebook sehr stark, während sie bei Google kaum bis gar nicht geäußert werden. Als Grund für die Nutzung von Facebook wird vor allem das große Netzwerk angegeben, welches einen in gewisser Weise dazu zwingt auch Teil des Netzwerks zu sein (T4, 125-128). Zwei Teilnehmer geben überdies an, immer Privatsphärebedenken zu haben, egal welchen digitalen Dienst sie nutzen, dass sie es aber akzeptieren

Datenspuren zu hinterlassen, um ein „Digital Player“ sein zu können. Ein anderer Teilnehmer bestätigt den Trend und hebt hervor, dass dieses Verhältnis immer mehr zunähme und, dass man häufig das Gefühl hat abgehört zu werden und Werbung basierend auf Mitschnitten privater Gespräche ausgesteuert zu bekommen (T6, 138-144). Diese Vermutung äußerten daraufhin alle Teilnehmer und nannten Beispiele, wie sie zuvor durch Abhörverfahren Zielgruppe für Werbeanzeigen geworden sind, oder aufgrund von Geo-Targeting mit Geschäften in Verbindung gebracht wurden, für die sie sich eigentlich nicht interessieren (T1-6, 151-189). Für alle gehen diese Praktiken zu weit, weshalb die Teilnehmer auch einen Blick auf ihre Einstellung der Ortungsdienste behalten (T3, 188-189).

Auf die Frage hin, ob Datenschutz den Teilnehmern wichtig sei, gab es unterschiedliche Meinungen. Es gab ein klares Ja (T6, 191), ein klares Nein (T5, 192) und zwei Stimmen die sagten, ihnen wäre Datenschutz wichtig, dass es aber widersprüchlich sei, weil sie ihre Daten nicht aktiv schützen würden (T3, T4, 193-198). Ein weiterer Teilnehmer sagte, dass er sich viel eher darauf verlasse, welche Daten er einpflegt, als zu überprüfen welchem Zweck die eigenen Daten dienen oder wer ihr Empfänger ist. So könne er die Praktiken der Industrie nachvollziehen man habe dann die Kontrolle, wenn man nur die Daten preisgebe, die man auch bereit ist preiszugeben (T1, 201-213). Der Teilnehmer, der sagte, dass ihm Datenschutz persönlich nicht so wichtig ist, äußerte in diesem Zusammenhang das Bedenken, dass einzelne Entscheidungen hierbei nicht immer entscheidend sind, sondern, dass die Gefahr darin bestehe, dass große Gruppen durch psychologisches Microtargeting politisch oder anderweitig instrumentalisiert werden könnten (T5, 216-222). Auf diese Erwähnung hin entsteht eine Diskussion, in der alle Teilnehmer ihr Bewusstsein äußern, dass enormer Einfluss über technische Mittel und digitale Dienste ausgeübt werden kann und das Geschmäcker und politische Meinungen nicht nur in den letzten Jahren durch geplante PR-Kampagnen gesteuert wurden (T1-6, 223-265). Aufbauend auf dieser Diskussion äußerte ein Teilnehmer die Hoffnung, dass solche Praktiken in Zukunft hoffentlich weniger würden und, dass über Regularien vielleicht etwas Ordnung in diesen Bereich gebracht werden könnte (T1, 270-280).

Nachdem die Teilnehmer einen tiefen Einblick in ihr Nutzerverhalten und ihre Privatsphärebedenken gegeben haben, wurde im weiteren Gesprächsverlauf auf technische Verfahren für Datenschutz und die Betroffenenrechte eingegangen. So wurde den Nutzern die Frage gestellt, ob sie bei Consent-Verfahren weitere Informationen über Cookies, Tracking und die Verwendung ihrer Daten lesen oder ob sie einfach zustimmen, um eine Website zu nutzen. Die Hälfte der Teilnehmer beantwortete die Frage mit der Aussage, Consent-Banner in der Regel immer mit OK zu beantworten, ohne die Informationen

abzufragen (T3, T4, T6, 289-291). Ein Teilnehmer gab an, dies seit der DSGVO nicht mehr zu tun, sondern von den Möglichkeiten Gebrauch zu machen, Datenschutzeinstellungen vorzunehmen, darunter Tracking-Verfahren, personalisierte Werbung und Cookies auszuschalten, wenn ein Consent-Layover erscheint (T2, 292-299). Ein weiterer Teilnehmer äußerte, dass er aktuelle Verfahren bezüglich des Cookies nicht komplett verstehe, da die Seite genauso nutzbar sei, egal ob man OK klicken würde oder nicht (T1, 293-295). Wie eine Einwilligung abläuft, dass man beim ersten Besuch für kommende Besuche einwilligt und, dass man die Privatsphäre Einstellungen auf Websites ändern kann, war einem Teilnehmer nicht wirklich bewusst (T3, 300-313). Es zeigt sich also, dass das Nutzerverhalten hier sehr stark variiert und das verschiedene Nutzertypen, mit möglichen unterschiedlichen technischen Hintergründen, nicht einheitlich abgeholt werden von Datenschutzrichtlinien und -möglichkeiten.

Die nächste Frage an die Teilnehmer betraf die Betroffenenrechte, speziell das Recht auf Auskunft, Berichtigung, Portabilität und Löschung. Hier wurden die Teilnehmer gefragt, ob sie von diesen Rechten Gebrauch machen würden. Alle Teilnehmer antworteten auf diese Frage bejahend. Hier herrscht besonders großes Interesse daran zu wissen, was Unternehmen wie Google über einen gespeichert haben (T4, T6, 327-332). Ein Teilnehmer würde auf jeden Fall sein Recht auf Löschung geltend machen, wenn er seinen Facebook Account löschen würde (T1, 336-337). Zwar gibt ein Teilnehmer an, Menschen zu kennen, die ihre Daten bereits einmal angefordert haben (T2, 333), auf die vertiefende Frage, ob einer der Teilnehmer dies bereits selbst getan hätte, folgt ein kollektives Nein (T1-T6, 343). Weiterhin wurde die Tendenz geäußert, dass man bei Facebook seine Daten löschen lassen würde, es bei Google aber keinen Sinn machen würde, da die eigene Nutzung zu hochfrequentiert sei (T2, 348-352).

Abschließend wurde die Frage gestellt, ob man denn für verstärkten Datenschutz bezahlen würde, bzw. dazu bereit wäre, Abstriche in der User Experience zu machen. Auf die Frage folgend entstand eine Debatte um die Monetarisierungsmodelle von digital agierenden Unternehmen. Zum einen gibt es großes Verständnis für die Datenverarbeitung als Geschäftsmodell (T2, T6, 373-381), zum anderen wurde geäußert man würde ein soziales Netzwerk oder eine Suchmaschine nicht mehr nutzen, sobald sie Geld kosten würde, oder man ginge zur Konkurrenz (T2, 377-381). Weiterhin benutzen einige Teilnehmer einen AdBlocker, um Werbeausspielung zu umgehen und besuchen eine Seite dann nicht, wenn der AdBlocker vom Websitebetreiber blockiert wird (T2, T4, 382-391). Ein Teilnehmer äußerte im Verlauf der Debatte, dass das aktuelle System ein Auslaufmodell sei und, dass es dahin gehen müsste, dass jeder Nutzer seine Daten selbst verwalte und man Mittelsmänner ausschalte (T1, 407-412). Abschließend wurde

geäußert, dass der technische Fortschritt stark von der Datenverarbeitung profitiert und, dass die Nutzer weiterhin Daten preisgeben müssen, um von dem Luxus, den Dienste wie Sprachsteuerung oder Smart Home Technology bieten, weiter profitieren zu können.

8.8 Der paradoxe Nutzer – Ein Profil

Aus der Gruppendiskussion lässt sich ein Nutzerprofil ableiten, welches sehr verbreitet zu sein scheint und in der Forschung bereits anteilig festgehalten wurde. Sowohl das kognitive Phänomen des Privacy Calculus, als auch des Privacy Paradoxons ließen sich bei der Fokusgruppe beobachten. Wir nennen dieses Nutzerprofil den paradoxen Nutzer. Dieser Nutzer verfügt durchaus über die nötige Kompetenz, einzuschätzen, dass er Datenspuren hinterlässt und einen Eingriff in seine informationelle Privatsphäre zulässt. Er äußert sogar explizite Bedenken, wann und wo Daten von ihm erfasst und verarbeitet werden, trotz einer nicht erteilten Einwilligung. Ebenfalls scheint dieser Nutzer kein zu großes Vertrauen in die Praktiken des sozialen Netzwerkes Facebook zu haben. Er wäre sogar bereit von seinen Betroffenenrechten Gebrauch zu machen, also aktiv und selbstbestimmt über seine Daten zu bestimmen und hat hierfür sogar konstruktive Vorschläge, wie das Marktsystem zu ändern sei.

Paradoxer Weise entscheidet sich dieser Nutzertyp dennoch meistens dazu, seine Einwilligung zur Datenverarbeitung zu erteilen, ohne zuvor die Datenschutzrichtlinie gelesen zu haben. Trotz einer Skepsis gegenüber Facebook, werden die persönlichen Informationen, das eigene Kontaktnetzwerk und die E-Mail-Adresse inflationär dazu verwendet, sich bei weiteren Anbietern zu registrieren. Die eigenen Daten und die der Freunde werden also mit multiplen Unternehmen geteilt und das meist aus Gründen der Bequemlichkeit. Weiterhin besitzt dieser Nutzertyp ein aktives Google Konto, welches er für digitale Anwendungen verschiedenster Lebensbereiche verwendet, trotz des Bewusstseins, dass Google hierdurch ein sehr genaues Datenblatt dieses Nutzers pflegen kann. Die in der DSGVO gestärkten Betroffenenrechte nimmt er sehr positiv wahr und äußert die Bereitschaft, diese auch aktiv anzuwenden, getan hat er dies jedoch noch nicht. Letztendlich hat er auch ein Verständnis für Online-Geschäftsmodelle und die Relevanz des Online-Werbemarktes, ist aber nur latent dazu bereit, Schutzvorkehrungen zu treffen, die zumindest den sensiblen Teil der eigenen personenbezogenen Daten zu schützen.

9 Handlungsempfehlungen

> „Während die Gewährsleute von Big Data sich bemühen, das Leben weiter zu verdaten, wird es umso dringlicher, zu verstehen, wie dieser Vorgang programmiert, algorithmisch berechnet, visuell repräsentiert und diskursiv modelliert wird (Reigeluth, 2015, S. 21)."

Nachdem die theoretisch hergeleiteten Forschungsfragen im Rahmen der qualitativen Befragungen geprüft wurden, können nun Handlungsempfehlungen für Nutzer und wirtschaftliche Akteure abgeleitet werden. Hierbei soll auf die in Kapitel 6 vorgestellten technischen Verfahren, Regulierungen und Nutzerrollen eingegangen und ihre Umsetzbarkeit mit den Erkenntnissen aus der empirischen Forschung verknüpft werden. Bevor auf die Selbstbestimmtheit und die Rolle des paradoxen Nutzers eingegangen wird, sollen zunächst die rechtlichen Auswirkungen der DSGVO aufgezeigt und Wege skizziert werden, wie Unternehmen unter Einhaltung der rechtlichen Vorgaben das Thema Datenschutz proaktiv mitgestalten können.

Wie aus der Auswertung der Experteninterviews abgleitet werden kann, sehen Akteure aus Wirtschaft und Rechtswesen eine Notwenigkeit zur Neugestaltung des Datenschutzrechts. Die DSGVO bildet hier einen geeigneten Grundstein, da sie ein harmonisiertes Recht für die gesamte Europäische Union darstellt und durch die hohen Strafen ausreichend Druck auf Unternehmen ausübt, die Inhalte umzusetzen und ihre Geschäftspraktiken DSGVO-konform umzustellen. Es zeigt sich aber auch die normative Unschärfe dieser Verordnung, da die DSGVO in ihrer Form zu generell ist, um dynamisch auf die komplexen Anwendungsbereiche datenbasierter Geschäftsmodelle reagieren zu können. So wird es für Akteure in der Online Marketing Branche eine Gratwanderung sein, zu entscheiden, welche Praktiken zweckgebunden bzw. erwartbar sind und dementsprechende Maßnahmen zu treffen. Letztlich gibt es aber gerade für Unternehmen, die im großen Stil Kunden- und Nutzerdaten sammeln und auswerten, Wege die Neuerungen einzuhalten und die Zukunft des Datenschutzes proaktiv mitzugestalten.

Aus ethischer Sicht sollte ein Unternehmen keine Daten erheben und verarbeiten, die es nicht für das operative Geschäft benötigt. Ebenfalls müssen datenbezogene Prozesse dokumentiert und die Auskunftsfähigkeit sichergestellt werden, um die Betroffenenrechte der Nutzer adäquat bedienen zu können und den Strafen der DSGVO zu entgehen. Im Zuge der DSGVO bereiten sich viele Markteilnehmer auf ein „consent based advertising" vor. Um auch weiterhin von den Daten der eigenen Nutzer profitieren zu können, gilt es, ein transparentes und intelligent eingebettetes Consent-Verfahren zu implementieren, welches Vertrauen für den Nutzer schafft und so wenig wie möglich die User Experience stört. Hier haben es Werbetreibende, kleinere Agenturen und Publisher

deutlich schwerer als die Tech-Riesen Google und Facebook, da sie mit Cookie Bannern und Overlays arbeiten müssen und von vielen Third Parties abhängig sind, während sich Facebook und Google ein einmaliges Opt-In für ihr gesamtes Ökosystem einholen können. Google und Facebook profitieren hier von ihrer großen Reichweite, den zuvor diskutierten Lock-In-Effekten und von der tiefen Verankerung im Alltag ihrer Nutzer. Die großen Marktplayer werden insoweit ihre Marktposition festigen können, auch wenn im Zuge der DSGVO mit Umsatzeinbußen zu rechnen ist. Um weiterhin konkurrenzfähig zu sein, müssen kleinere Marktteilnehmer das Thema Privatsphäre und Datenschutz neudenken und innovative Wege finden oder unterstützen, die den Nutzer stärker an der Wertschöpfung beteiligen und über diese aufklären. Hierbei gilt es den technologischen Fortschritt nicht zu beschneiden, sondern dem Nutzer mehr Anreize zu bieten, von seinen eigenen Daten zu profitieren. Wichtig ist, dass Nutzer nur solche Daten preisgeben, die sie bereit sind mit Dritten zu teilen oder die keinen Personenbezug zulassen.

Die sowohl von einem Teilnehmer der Gruppendiskussion vorgeschlagene, als auch von dem Datenschutzexperten Stecher vorgestellte Einführung eines Daten-Portemonnaies, wäre ein geeigneter Weg alle Parteien selbstbestimmt agieren zu lassen, ohne den technologischen Fortschritt zu beschneiden. Hier könnte jeder Nutzer seine Daten hinterlegen, die er bereit ist preiszugeben. Den Zugriff auf diese Daten durch Unternehmen kann er so transparent einsehen und kontrollieren. Nutzer würden nach wie vor Datenspuren hinterlassen, jedoch in einem ethisch vertretbaren Rahmen, da sie souverän und selbstbestimmt ihre Daten und die Zugriffe darauf verwalten könnten. Das Phänomen des Privacy Paradoxons und die Trägheit vieler Nutzer lässt sich jedoch als Gegenargument für diesen Weg aufführen, da er von einer starken Partizipation der Nutzer abhängt. Es ist nicht zu erwarten, dass jeder Nutzer sich regelmäßig die Mühe macht, seine Daten einzupflegen, zu aktualisieren, zu berichtigen, zu löschen, zu kategorisieren und je nach Verwendungszweck freizugeben. Der Weg, die Nutzer so kompetent und selbstbestimmt auszustatten, dass sie diese Aufgabe adäquat ausüben können, wird sich nur schwer oder über einen langen Zeitraum realisieren lassen.

Die Nutzer sollten nicht durch Bevormundung und nur scheinbare Selbstbestimmtheit zur eigenen Beschneidung ihrer User Experience oder zur Aufgabe ihrer Privatsphäre für das beste Angebot getrieben werden, sondern als aktiver Teilnehmer in Datentransaktionen einbezogen werden. „Eine Politik der reinen Verbrauchererziehung (etwa in Richtung Datensparsamkeit) erscheint aus ökonomischer Sicht kaum angebracht, da sie die schon vorhandene Unsicherheit der Verbraucher nur vergrößert, aber keine institutionellen Rahmenbedingungen schafft, die mehr Datensicherheit bieten (Dold & Krieger, 2016, S. 6).“ Der erste Schritt, den Nutzer zu einer echten Selbstbestimmtheit zu

ermächtigen, ist die nötige Kompetenz zu schaffen. Dieser Prozess muss sowohl im Bildungssystem als auch in Unternehmen implementiert werden. Sobald jeder Nutzer in der Lage ist, einzuschätzen, wo und wann er welche Daten preisgibt, kann er selber entscheiden, wie weit er von datengetriebenen Diensten profitieren möchte. Es wäre fatal, wenn ein Großteil der Convenience und der positiven User Experience zu Lasten des Datenschutzes verloren gehen würde. Der Datenschutz muss zwar verstärkt, seiner Unschärfe bereinigt und weiter aufgegliedert werden, er darf aber nicht digital mündige Nutzer in ihrem Nutzerverhalten einschränken.

Also halten wir fest, dass sich das System zumindest in näherer Zukunft nicht vollends umwälzen lässt, ohne den Markt, Geschäftsmodelle oder den Fortschritt zu beschneiden. Wie sorgt man also für verstärkte Datensicherheit und die Einhaltung ethischer Grundsätze in der Datenverarbeitung? Die DSGVO ist hier in ihrer Form akzeptabel und als Schritt in die richtige Richtung zu sehen. Sie wird wohl dazu führen, dass Consent-Verfahren inflationär zum Einsatz kommen, Unternehmen aber sobald sie den Opt-In der Nutzer haben, fast genauso intransparent Daten verarbeiten können wie zuvor. Probleme wie Intransparenz, ethische Bedenken, Datenschutz und -verarbeitung und die Umgehung von Regulierungen und Selbstregulierungen sind Verantwortlichkeiten, denen Unternehmen bereits Rechenschaft ablegen müssen. Besitzrechte von Daten hingegen sind ein gänzlich neues Feld (Grigore, Molesworth, & Watkins, 2017, S. 107). Die Einführung einer Corporate Digital Responsibility, die Unternehmen einzuhalten haben, wäre als weiterer und umso wirksamerer Schritt anzusehen. Unternehmen müssten intern überprüfen, dass der Umgang mit Daten ethisch korrekt verläuft und könnten sich darüber hinaus sogar am Markt mit Datensicherheitsversprechen positionieren.

Letztlich darf die Rolle der Nutzer nicht vergessen werden. Aus den Inhalten der Gruppendiskussion ist abzulesen, dass sich die kognitiven Prozesse des Privacy Calculus und des Privacy Paradoxons bestätigen lassen. Nutzer äußern also ihre Privatsphärebedenken und lassen diese in die Entscheidung zur Nutzung digitaler Dienste einfließen, entscheiden sich jedoch inflationär für die komfortabelste Lösung. Das ist auf der einen Seite nachvollziehbar, auf der anderen Seite aber auch alarmierend, da die wachsenden Datenmengen mit der steigenden Internetnutzung (Initiative D21, 2018, S. 10) korrelieren. Hierdurch bleibt dem Nutzer weniger Zeit, seine Rolle in digitalen Geschäftsmodellen zu hinterfragen. Weiterhin zeigt sich, dass die meisten Nutzer nicht auf die Vorteile, die ihnen datengetriebene Dienste ermöglichen, verzichten wollen, obwohl ihr Vertrauen in Unternehmen wie Facebook geringer wird. Nutzer machten bisher nicht viel Gebrauch von ihren Betroffenenrechten und auch die Experten äußern, dass Nutzer auch in Zukunft nicht vermehrt auf diese zurückgreifen werden. Dennoch schaffen diese Vertrauen

beim Nutzer und werden als positives Mittel zur informationellen Selbstbestimmtheit wahrgenommen.

Die Kompetenz der Nutzer wird größer (Initiative D21, 2018, S. 8), die DSGVO übt Druck auf die Unternehmen aus, ihre Prozesse und Technologie datenschutzrechtskonform anzupassen und zu entwickeln, und in der Branche entstehen Verfahren, die das Ziel verfolgen einen faireren Umgang mit Daten zu realisieren. Wie kann man letztlich die Einstellungen und Bedürfnisse der Nutzer mit den Anforderungen des Marktes, Datensicherheit und Fortschritt in Einklang bringen? Die Zukunft wird zeigen, ob der Spagat gelingt und man Nutzer und Unternehmen gleichermaßen an der Wertschöpfung der Verarbeitung von personenbezogenen Daten partizipieren lassen kann. Wichtig wird sein, dass das Thema weiterhin im öffentlichen Diskurs bleibt, denn radikale Änderungen wird es auch mit der DSGVO nicht geben. Was bleibt ist ein Appell.

10 Bestimmt über eure Daten! - Ein Appell an Nutzer und Unternehmen

Im Verlauf dieser Arbeit wurden Daten als das Erdöl des 21. Jahrhunderts bezeichnet. Anders als beim Erdöl zeigt sich jedoch nicht die Knappheit der Ressource, sondern das ungebremste Ansteigen an Datenmengen als Gefahr und als Ursprung für ein Umdenken im Umgang mit diesem wertvollen Gut. Die eigentlichen Produzenten der Ressource Daten sind die Nutzer. Die Konzerne verarbeiten diese zwar und bereiten sie auf, der tatsächliche Wert ist aber in seinem Ursprung auf einzelne, bestimmbare Individuen zurückzuführen. Datenschutz ist von enormer Bedeutung in der heutigen digitalen Welt, Datensicherheit muss das höchste Gut im Umgang mit Daten von Unternehmen sein und der digitale Fortschritt sollte aus ökonomischer Sicht nicht gebremst werden. Doch um alle diese Komponenten zu berücksichtigen und in Einklang zu bringen, muss der Nutzer an der Wertschöpfung beteiligt werden. Man sollte Nutzern nicht vorenthalten, dass sie in Form ihrer persönlichen Daten über einen enormen Wert verfügen, welchen sie selbstbewusst und gewinnbringend veräußern können. Auf der anderen Seite müssen sich die Nutzer aktiv in einen Veränderungsprozess einbringen. Betroffenenrechte, wie sie in der DSGVO enthalten sind, müssen von den Nutzern mit Leben gefüllt werden. Der große Einfluss den Facebook und Google auf ihre Nutzer ausüben können, kann invertiert werden, sodass die Nutzer in ihrer Masse Druck auf die Konzerne ausüben können. Die Werkzeuge, die die Nutzer hierfür brauchen, haben die großen Netzwerke für sie bereits gebaut (Weigend, 2017, S. 227).

Es geht hierbei nicht darum eine Revolution anzustoßen, die Datenstränge zu kappen und den großen Tech-Konzernen zu schaden. Suchmaschinen, Smart Technology oder Personalisierung werten unseren Alltag in verschiedensten Bereichen auf. Wir können in Zukunft von diesen Technologien und unseren Daten nur profitieren, wenn ihre Verarbeitung nachhaltig und ethisch vertretbar ist. Nutzer sollten ihre Daten selbstbestimmter verwalten. Wenn sie dazu nicht bereit sind, muss das Recht und die Unternehmensethik sie auffangen und schützen. Der Nutzen für den Konsumenten darf nicht nur ein leeres Marketing-Versprechen sein und seine Aufmerksamkeit und seine Bewegungen nur dazu genutzt werden, Werbekontakte, Klicks und Conversions zu generieren, um auf dem Werbemarkt Umsätze zu erzielen. Es ist anzunehmen, dass Nutzer gerne Inhalte und auch persönliche Informationen teilen, wenn ihnen der Nutzen dafür transparent vermittelt wird. Gegen intelligente Algorithmen, die Nutzern personalisierte Inhalte und Anzeigen zuordnen, werden digital aufgeklärte Nutzer keinen Einwand haben. Wenn sie dies nicht wollen, müssen sie aber auch in der Lage sein können, ihre Datenstränge komplett zu kappen und nicht nur diejenigen, die eine hohe digitale Kompetenz mitbringen. Die DSGVO ist ein Schritt in die richtige Richtung. Die Umsetzung eines

effizienteren Systems für den Datenmarkt muss von Unternehmen, Visionären und letztendlich von den Nutzern selbst entwickelt werden.

Literaturverzeichnis

Athey, S., Catalini, C., & Tucker, C. (2017). T*he Digital Privacy Paradox. Small Money, Small Costs, Small Talk.* (S. I. Research, Hrsg.) Stanford, California, United States of America.

Bellman, B. L. (1981). *The Paradox of Secrecy.* In B. L. Bellman, Human Studies 4. La Jolla, California, United States of America: Department of Sociology, University of California, San Diego .

Brave (2018). *Brave Browser*. Abgerufen im Juli 2018 von https://brave.com/

Bruns, A., Dang-Xuan, L., Neuberger, C., & Stieglitz, S. (2014). *Social Media Analytics. An interdisciplinary approach and its implications for information systems.* Business & Information Systems Engineering, S. 89-95.

Buck, C., Stadler, F., Suckau, K., & Eymann, T. (7. Dezember 2016). *Nutzer präferieren den Schutz ihrer Daten*. *HMD*, S. 55-66.

Charlesworth, A. (2018). *Digital Marketing. A practical Approach.* New York, NY, United States of America: Routledge.

Danwitz, T. v. (September 2015). *Die Grundrechte auf Achtung der Privatsphäre und auf Schutz personenbezogener Daten.* Datenschutz und Datensicherheit, S. 581-585.

Deuker, A. (2010). *Addressing the Privacy Paradox by Expanded Privacy Awareness – The Example of Context-Aware Services.* Privacy and Identity. (M. Bezzi, Hrsg.) Frankfurt a.M., Hessen, Deutschland.

Dold, M., & Krieger, T. (2016). *Informationelle Selbstbestimmung aus ordnungsökonomischer Sicht.* Freiburg, Baden-Württemberg, Deutschland: Wilfried- Guth-Stiftungsprofessur für Ordnungs- und Wettbewerbspolitik.

Eling, N. (2017). *Der Wert von Nutzerinformationen aus Anbieter- und Nutzerperspektive. Analyse des Trade-offs zwischen Datenverwendung und Datenschutz.* Wiesbaden: Springer Gabler.

Epping, V. (2017). *Grundrechte.* Hannover: Springer-Lehrbuch.

Ernst, C.-P. H. (2014). *Factors Driving Social Network Site Usage.* Wiesbaden, Hessen, Deutschland: Springer Gabler.

European Commission (9. Juni 2018). *European Commission. Information Providers Guide. The EU Internet Handbook*. Von http://ec.europa.eu/ipg/basics/legal/cookies/ abgerufen

Facebook (2012). *Facebook annual report 2012*. Abgerufen im Juli 2018 von Facebook Investor Relations: https://s21.q4cdn.com/399680738/files/doc_financials/annual_reports/FB_2012_10K.pdf

Facebook (31. 12 2017). *Facebook Q4 2017 Results.* Abgerufen im Juli 2018 von Facebook Investor Relations: https://investor.fb.com/financials/default.aspx

Facebook (2018). *Facebook Q1 2018 Results.* Abgerufen im Juni 2018 von Facebook: https://s21.q4cdn.com/399680738/files/doc_financials/2018/Q1/Q1-2018-Earnings-Presentation-(1).pdf

Ferguson, N. (2017). *Türme und Plätze.* London: Pengui Books.

Galloway, S. (2017). *the four. The hidden DNA of Amazon, Apple, Facebook, and Google.* New York, New York, USA: Penguin Random House LLC.

Gerber, P., Volkamer, M., & Gerber, N. (2017). *Das Privacy-Paradoxon – Ein Erklärungsversuch und Handlungsempfehlungen.* In D. D. (Hrsg.), & D. D. e.V. (Hrsg.), Dialogmarketing Perspektiven 2016/2017. Tagungsband 11. wissenschaftlicher interdisziplinärer Kongress für Dialogmarketing. Wiesbaden: Springer Gabler.

Gläser, J., & Laudel, G. (2014). *Expertenintervires und qialititative Inhaltsanalyse.* Wiesbaden: VS Verlag für Sozialwissenschaften | Sringer Fachmedien Wiesbaden GmbH.

Grigore, G., Molesworth, M., & Watkins, R. (2017). *New Corporate Responsibilities in the Digital Economy.* In A. Theofilou, Georgiana Grigore, & A. Stancu, Palgrave Studies in Governance, Leadership and Responsibility. Cham, Switzerland: Springer International Publishing AG.

Härting, N. (2016). *Datenschutzgrundverordnung. Das neue Datenschutzrecht in der betrieblichen Praxis.* Köln: Verlag Dr. Otto Schmidt KG.

Hornung, G., & Herfurth, C. (2018). *Datenschutz bei Big Data – Rechtliche und politische Implikationen*. In C. König, J. Schröder, & E. Wiegand, Big Data. Chancen, Risiken und Entwicklungstendenzen. Wiesbaden: Springer VS .

Horstmann, U. (2018). *Digitale Knechtschaft. Wie wir von Konzernen und Staaten gesteuert werden.* (Bd. 1). München: Redline Verlag, ein Imprint der Müchner Verlagsgruppe GmbH.

Initiative D21 (2018). *D21 Digital Index 2017/2018. Jährliches Lagebild zur Digitalen Gesellschaft.* Abgerufen im Juni 2018 von initiatived21: https://initiatived21.de/app/uploads/2018/01/d21-digital-index_2017_2018.pdf

Interactive Advertising Bureau (25. April 2018). *Interactive Advertising Bureau Europe*. Abgerufen im Juli 2018 von Transparency & Consent Framework specification launches global as industry participation increases: https://www.iabeurope.eu/blog/blog-transparency-consent-framework-specification-launches-global-as-industry-participation-increases/

Intersoft Consulting (25. Mai 2018). *Personenbezogene Daten (DSGVO)*. Abgerufen im Mai 2018 von DSGVO. Datenschutz-Grundverordnung: https://dsgvo-gesetz.de/themen/personenbezogene-daten/

Intersoft Consulting (25. Mai 2018). *Privacy by Design (DSGVO)*. Abgerufen im Mai 2018 von DSGVO. Datenschutz-Grundverordnung: https://dsgvo-gesetz.de/themen/privacy-by-design/ abgerufen

Jentzsch, N. (2014). *Monetarisierung der Privatsphäre: Welchen Preis haben persönliche Daten?* Berlin, Berlin, Deutschland.

Jung, A. (06 2018). *Die Datenschutzformel - Vom Atmen und der Beatmung des Datenschutzes.* MMR. Multimedia und Recht. Zeitschrift für Informations-, Telekommunikations- und Medienrecht, 349-350.

Kamps, I., & Schetter, D. (2018). *Performance Marketing. Der Wegweiser zu einem mess- und steuerbaren Marketing - Einführung ind Instrumente, Methoden und Technik.* Wiesbaden: Springer Gabler.

Lee, B.-K., & Lee, W.-N. (2004). *The Effect of Information Overload on Consumer Choice Quality in an On-Line Environment.* Psychology & Marketing (21/3), 159-183.

Mühlichen, A. (2014). *Informationelle Selbstbestimmung.* In N. Baur, & J. Blasius, Handbuch Methoden der empirischen Sozialforschung. Wiesbaden: Springer Fachmedien.

MyData (2018). *MyData*. Abgerufen im Juli 2018 von What We Want: https://mydata.org/declaration/german/

Nocun, K. (2018). *Die Daten, die ich rief.* Köln: Bastei Lübbe AG.

OECD (2016). *OECD Recommendation of the Council on Consumer Protection in E-Commerce*. Paris, Frankreich.

Petrlic, R., & Sorge, C. (2017). *Datenschutz. Einführung in technischen Datenschutz, Datenschutzrecht und angewandte Kryptographie.* Wiesbaden: Springer Vieweg.

Reichert, R. (Februar 2015). *Digitale Selbstvermessung Verdatung und soziale Kontrolle.* Zeitschrift für Medienwissenschaft. 13 Überwachung und Kontrolle, S. 66-77.

Reigeluth, T. (Februar 2015). *Warum Daten nicht genügen. Digitale Spuren als Kontrolle des Selbst und als Selbstkontrolle.* Zeitschrift für Medienwissenschaft. 13 Überwachung und Kontrolle, S. 21-34.

Scholl, A. (2003). *Die Befragung.* Konstanz: UVK Verlagsgesellschaft mbH.

Selke, S. (2016). *Lifelogging. Digitale Selbstvermessung und Lebensprotokollierung zwischen disruptiver Technologie und kulturellem Wandel.* Wiesbaden: Springer Fachmedien.

Smith, H. J., Dinev, T., & Xu, H. (2011). *Information Privacy Research: An Interdisciplinary Review.* University Park, PA: Pennsylvania State University.

Vogl, S. (2014). *Gruppendiskussion.* In N. Baur, & J. Blasius, Handbuch Methoden der empirischen Sozialforschung. Wiesbaden: Springer fachmedien.

Voigt, P., & Bussche, A. v. (2018). *EU-Datenschutz- Grundverordnung (DSGVO). Praktikerhandbuch unter vollständiger Berücksichtigung des deutschen Datenschutz-Anpassungs- und -Umsetzungsgesetzes EU (DSAnpUG-EU).* Berlin: Springer Verlag GmbH.

Wass, C., & Kurz, T. (10 2012). *Digitale Hilfsmittel für mehr Transparenz bei der Verarbeitung personenbezogener Daten.* Datenschutz und Datensicherheit, S. 748–752.

Weigend, A. (2017). *Data for the people. Wie wir die Macht über unsere Daten zurückerobern.* Hamburg: Murmann Publishers GmbH.

Werner, K., & Buttlar, H. v. (28. Juni 2018). *Capital*. Abgerufen am Juli 2018 von https://www.capital.de/wirtschaft-politik/das-jaehe-ende-der-tech-euphorie?article_onepage=true

Will, M. G. (2015). *Privacy and Big Data: The Need for a Multi- Stakeholder Approach for Developing an Appropriate Privacy Regulation in the Age of Big Data.* Halle, Sachsen-Anhalt, Deutschland.

X Anhang

X.I Experteninterview 1

Do. 31.05.2018, 16:00 Uhr, Hamburg

Ilka Voss

Teamleiterin Online Marketing • Real Time

OTTO GmbH & CO. KG

Begrüßung des Interviewpartners, kurze Vorstellung der Master Thesis und Einholung einer Einwilligung zur Aufzeichnung und Veröffentlichung des Leitfadeninterviews.

Florian Kugler: Die ersten Fragen thematisieren die Relevanz der DSGVO. Hältst du eine neue Gesetzgebung hinsichtlich Datenschutz für notwendig? Im Generellen.

Ilka Voss: Ja, auf jeden Fall. Ich denke die alte Gesetzgebung bezüglich der digitalen Weiterentwicklung der Welt, sag ich mal, überhaupt nicht mehr angepasst war. Insofern finde ich es absolut richtig, dass ein neues Gesetz in Kraft tritt, ja.

Florian Kugler: Ok. Denn die letzte ist ja über 25 Jahre her und hat deswegen noch nicht die heutige Praxis, die Praktiken im Online Marketing beinhaltet. Also welche konkreten Auswirkungen der DSGVO auf Online-Marketing-Prozesse erwartest du?

Ilka Voss: Ja ich glaube es gibt Implikationen, direkte, aber eher bezüglich Daten… Also was komplizierter wird, ist ja die Datenverarbeitung, also bei unserer Seite auch, dass wir Daten verschlüsseln, nicht mehr Daten solange halten können, das die Zeiten auch verkürzt werden, aber im Grunde genommen was ich meine, wir können Daten nach wie vor so nutzen, wie vorher, bloß die Datenverarbeitung und die Datenhaltung ändert sich für mich so ein bisschen. Und die Möglichkeit zu geben, ja also in dem Moment schon, wenn man weißt es geht um Informationspflichten, den man nachkommen muss oder Löschungspflichten, das ändert sich dann in dem Sinne, das heißt in der Nutzung für mich im ersten Schritt mit der DSGVO nicht, im Zusammenspiel mit der Cookie Richtlinie, also die heute noch gilt, ja.

Florian Kugler: Du hast es ja schon ein bisschen beantwortet, welche Auswirkungen wird die DSGVO dann auch speziell auf programmatischen Einkauf, auf Retargeting, Tracking und Profiling basierte Targetings haben, also sind da Auswirkungen zu erwarten oder greift es wirklich eher nur auf die Betroffenenrechte zu und auf die Dokumentationspflichten?

Ilka Voss: Aus mein Sicht ja, aber im Zusammenspiel mit der E-Privacy Verordnung, die dann ja auch ansteht, ist es dann ein Gesamtpaket, was natürlich sich heute, was absehbar ist, was Auswirkungen auf das Online-Marketing haben wird, weil dann in dem

Moment, also ich sehe es so, die Datenschutzgrundverordnung ist der Grundbaustein, da geht es um Datenverarbeitung und wie hast du es eben genannt?

Florian Kugler: Betroffenenrechte

Ilka Voss: Betroffenenrechte, sozusagen, denen gerecht zu werden, aber die weitere Ausführung dann, bezüglich auf neue Kommunikationskanäle und Trackingmethoden, das ist ja die e-Privacy Verordnung, die dann kommt und das ganze ergänzt. Und es zeichnet sich halt ab, dass da große Veränderungen anstehen, also aus einem Opt-Out ein Opt-In wird, wir also die Einwilligung des Nutzers brauchen, wenn wir die Daten verarbeiten wollen, Profile erstellen wollen und diese für Werbezwecke nutzen wollen. Und das ist für mich die große Veränderung die ansteht, die sich besonders auf das Online-Marketing auswirkt. Nur die DSGVO alleine, sag ich mal, so aus meiner Sicht, schränkt es nicht ein, es ist mehr Aufwand erforderlich, um mit den Daten zu arbeiten, aber im Grunde genommen außer jeder Nutzer kommt… Also der Worst Case wäre jetzt, „löscht meine Daten“, alle stehen jetzt hier Schlange bei OTTO und sagen sie möchten, dass ihre Daten gelöscht werden. Das passiert ja momentan nicht, ich glaube das wird auch nicht in dem Sinne bemerkbar sein.

Florian Kugler: Also ein Opt-In ist nicht für alle Praktiken von Nöten durch die DSGVO, ist aber im Zuge e-Privacy Verordnung zu erwarten?

Ilka Voss: Genau, also für das was die DSGVO vorschreibt ist das Opt-In da ja nicht festgehalten, sondern es verweist ja sozusagen eigentlich genau da in dem Kontext auf die e-Privacy Richtlinie beziehungsweise auf die Verordnung, die dann kommen wird. Da ist es zu erwarten und dann sind die Implikationen ganz andere.

Florian Kugler: Die großen Unternehmen wir Google zeigen sich da ja schon proaktiv und holen jetzt trotz keiner direkten Verpflichtung durch die DSGVO, trotzdem schon den Opt-In häufig von Usern ein. Dazu stellt sich die Frage, also wird sich DSGVO oder die kommende e-Privacy Verordnung positiv oder negativ auf die Marktmacht der großen Unternehmen auswirken, kann es sein, dass sie ihnen in die Karten spielen, dass sie hierdurch ihre Marktmacht weiter ausbauen können, oder ist es sogar ein Hindernis?

I**lka Voss:** Ich sehe schon, dass da die großen Marktplayer einen Vorteil haben, also gerade Google und Facebook, weil sie für sich natürlich heute schon auf Grund einer Monopolstellung, muss man fast sagen, oder sie bieten ein Produkt an, was letztendlich dann wo sie ja heute die Oft-Ins einsammeln, um dieses Produkt zu nutzen. Das ja ein Kopplungsverbot also nach vorne wäre, aber heute macht das Facebook ja, man kann ja eigentlich nur da rein, wenn man sich einloggt, und mit dem Einloggen stimme ich bestimmten Datenschutzrichtlinien zu. Da haben sie natürlich eine Monopolstellung, weil sie ein Produkt, auf welches die Nutzer nicht verzichten wollen, dass sie eben ihr Opt-In geben. Bei Google genauso, bei der Google Suche zum Beispiel, ich hätte eine Alternative schon im Markt, aber den Nutzern ist es nicht bewusst, was sie dort eigentlich tun

und sie willigen dort auch ein, sie loggen sich ein und durch die Vielfalt der Google Produkte, Google Mail zu nutzen, hat Google einfach die Möglichkeiten Daten zusammenzuführen und sich das Opt-In zu holen, und ist da auf jeden Fall dem Markt voraus. Hat da definitiv im Wettbewerb gewonnen. Während die anderen Unternehmen in Deutschland, also aus OTTO Perspektive auch, ist es natürlich schwierig zu sagen, kann man sich keinen Opt-In erzwingen, man kann ja die Nutzung des Shops nicht davon abhängig machen, dass der Nutzer mir sein Opt-In gibt, weil er da zu viele Möglichkeiten im Markt hat, also Alternativen woanders hinzugehen.

Florian Kugler: Also das Kopplungsverbot sagt ja auch eigentlich, dass eine Verknüpfung von Daten, die jetzt nicht in direktem Zusammenhang mit einem Vertragsschluss stehen, dass es nicht rechtmäßig wäre, diese Daten trotzdem zu erheben. Umgehen das Google und Facebook in gewisser Weise?

Ilka Voss: Aus meiner Sicht schon. Es verstößt absolut gegen das Kopplungsverbot, was sie heute betreiben. Also Facebook insbesondere und das ist glaube ich ein Punkt wo die Datenschutzbehörden schon bei Facebook dran sind aber worüber sie sich einfach hinwegsetzen, weil sie eben kein europäischer Player, sondern ein amerikanischer Player, wo es letztendlich andere Grundlagen gibt oder wo das eben kein Problem ist.

Florian Kugler: Generell würdest du sagen, dass die DSGVO zu kurz greift oder schon zu weit geht in ihren Ausformulierungen?

Ilka Voss: Die DSGVO finde ich greift nicht zu weit, ich glaube das was sie da tun, das passt so finde ich, es ist ein großer Mehraufwand bei den Unternehmen, der dadurch entsteht. Die Frage ist was will der Nutzer eigentlich, also hat man den Nutzer im Vorfeld eigentlich konkret mal gefragt, was sind die wirklichen Ängste oder was treibt sozusagen, dass ich diese Datenschutzgesetzgebung ausbaue. Aus Nutzerperspektive will ich eine Transparenz dafür haben oder sicher gehen, dass nicht zu viele Daten erhoben werden. Das ist ja das was mich (als Nutzer) treibt und dass ich die Möglichkeit hätte Einblick zu bekommen, was machen die denn mit meinen Daten und das finde ich deckt die DSGVO gut ab, vielleicht ein bisschen zu viel des Guten und dadurch der große Aufwand für die Unternehmensseite. Die Frage ist ob dieser gerechtfertigt ist? Also ob der Nutzer das wirklich will, was da gerade alles passiert? Kann ich aus Nutzersicht gar nicht sagen. Inwiefern der Durchschnittsnutzer, was ist ihm wirklich wichtig, was braucht er?

Florian Kugler: Die Nutzerperspektive steht bei de DSGVO ja sehr im Vordergrund. Siehst du die DSGVO auch als Chance für Unternehmen? Sich vielleicht in ihren Marktbemühungen zu verändern, sich vielleicht weiterzuentwickeln?

Ilka Voss: Als Chance? Vielleicht schon. Bei Otto haben wir schon die Situation, dass bei Otto der Datenschutz immer eine große Rolle gespielt hat, man könnte sich natürlich im Markt stärker damit positionieren. Bei uns sind die Daten sicher, bei uns hast du die Transparenz, das wäre eine mögliche Chance. Das wäre eine Möglichkeit.

Florian Kugler: Also können Unternehmen da auch proaktiv die Zukunft mitgehalten?
Ilka Voss: Die Zukunft nicht mitgehalten aber vielleicht das Momentum, dass da gerade ein Fokus draufgelegt wird. Bei uns wird Datenschutz großgeschrieben, bei uns kannst du dir sicher sein, dass wir mit deinen Daten richtig umgehen und die Gesetze einhalten. Das darüber auch beim Nutzer punkten kannst. Ich weiß bloß garnicht, wie wichtig das dem Nutzer überhaupt ist? Man sagt es immer, und es ist auch das was so betrieben wird, alle wollen Transparenz haben und den Datenschutz hochschrauben, aber gleichzeitig geben sie ihre Datenschutzrechte komplett bei Facebook und bei Google ab. Und das tun sie einfach so. Ich glaube es ist so eine Range von sehr anspruchsvoll sein in dem Bereich bis „mir ist es egal was die machen mit meinen Daten“ und das auszutarieren, ich glaube es besteht eine Chance aber wie groß ist die Zielgruppe, die wirklich darauf anspringen, ja bei dem Unternehmen kaufe ich. Alternative ist Amazon und Otto. Kaufen sie jetzt bei Amazon nicht mehr weil sie da anders mit den Daten umgehen als bei OTTO? Bezweifle ich, da ist jeder sich der Nächste, also dann zahle ich doch lieber 2€ weniger für ein Produkt und bestelle bei Amazon.
Florian Kugler: Das ist gerade das was die DSGVO möchte, die Betroffenenrecht zu stärken, dem Nutzer eigentlich mehr Werkzeuge an die Hand zu geben, selbstbestimmter mit den eigenen Daten umzugehen oder darüber überhaupt selbstbestimmt zu sein. Deswegen kommen wir jetzt auch zur Nutzerperspektive. Also welche der Rolle nimmt der Nutzer in Zukunft ein? Oder wie wirkt sich das auch auf das Nutzererlebnis aus. Eine eher technische Frage die sich erstmal direkt stellt ist: Glaubst du, dass viele Nutzer den Opt-In verweigern werden, beziehungsweise aktuell noch den Opt-Out wählen?
Ilka Voss: Ich glaube ja, wenn es die Möglichkeit gibt darüber zu entscheiden. Es ist schwierig abzuschätzen aber wir werden sicherlich nicht 100% Opt-In haben, das werden wir definitiv nicht haben und ich finde realistisch sind schon 50% und vielleicht auch realistisch irgendwo zwischen 50 und 100% zu landen, wenn der Nutzer sich daran gewöhnt hat und die Vorteile darin sieht gegebener Weise einen Opt-In zu wählen und das ist glaube ich die große Herausforderung, zu zeigen es lohnt sich einen Opt-In zu geben, weil du dann gewisse Vorteile hast. Also wie es heute schon getan wird, das gewisse Rabatte gelten oder es eine Incentivierung gibt, die darf natürlich nicht gekoppelt sein aber im Grunde genommen zu einem Kreis zu gehören, der besondere Angebote bekommt. Darum geht es ja.
Florian Kugler: Die nächste Frage geht genau in die Richtung. Würden die Nutzer ihre Betroffenenrechte in Zukunft stärker ausnutzen …
Ilka Voss: …das glaube ich nicht…
Florian Kugler: … oder geben sie ihre Selbstbestimmung für Nutzung von Diensten und möglicherweise Vorteile, wie Rabatte, dann doch sehr leichthändig auf?

Ilka Voss: Ich glaube schon, dass die Nutzer eigentlich träge sind und dass ihnen das alles eigentlich viel zu anstrengend ist sich damit jetzt spezifisch auseinanderzusetzen. Also wo gebe ich meinen Opt-In, wo gebe ich das jetzt nicht. Das überfordert den normalen User aus meiner Sicht und auch die Betroffenenrecht beim Unternehmen anzufragen… also das stimmt nicht ganz, wenn ich das mal eben per Klick machen kann, dann mache ich das so, aber wenn ich einen Brief oder eine E-Mail schreiben muss und an ein Unternehmen herantrete und sage, „so kannst du mir jetzt mal zeigen, was du alles mit meinen Daten machst", dann glaube ich werden das ganz wenige tun. Bei Google ist es glaube ich möglich mittlerweile, dass man gucken kann wo werden meine Daten wie verarbeitet, aber auch das macht man einmal und dann macht man es nicht mehr. Ich glaube nicht, dass das die Nutzer in diesem Maße für sich in Anspruch nehmen oder dann nutzen werden, dass es den Aufwand rechtfertigt, der dahintersteht.

Florian Kugler: Nun ist ja auch Privacy by Design und Privacy by Default Inhalt der DSGVO und damit sollen ja schon technisch Grundlagen gelegt werden, dass Oberflächen so gestaltet werden, dass eine hohe Privatsphäre bereits eine Grundeinstellung ist, eine die Privatsphäre schützende Voreinstellung.

Ilka Voss: Das finde ich sehr kritisch. Man schafft damit Tatsachen, die den Nutzer auch wirklich überfordern. Also eine Privacy by Default Einstellung in einem Browser erfordert ja eine Rückeinstellung durch den Nutzer. Ich glaube die meisten Nutzer sind sich nicht der Komplexität und der Folgen bewusst, was das eigentlich bedeuten würde. Das gegebenenfalls auch Personalisierungsmaßnahmen einfach unterbunden werden und, dass es ja schon auch Vorteile für den Nutzer hat, wenn er die Wahl hat. Und ich glaube die Wahl hat er nicht mehr dann, wenn es eine Voreinstellung ist. Diese Voreinstellung zurückzudrehen ist für viele Nutzer gar nicht möglich, weil sie gar nicht wissen, wie sie es tun sollen. Weil sie gar nicht wissen, dass sie eine Browsereinstellung vornehmen können. Also das ist eine gewisse Anzahl von Nutzern in Deutschland, eine Zielgruppe die kann das, weil sie eine technische Affinität hat oder sich damit auseinandersetzt. Das Gros der Nutzer weiß aber nicht wie das funktioniert. Und da finde ich ist es der falsche Weg, und vor allem in dem Kontext, dass man den Browsern damit die Vormachtstellung gibt, dass die Browser, weil sie diese Grundeinstellung haben. Die Browser sind ja nicht losgelöst von irgendwelchen Unternehmen, sondern die hängen ja auch bei Google mit drin, bei Microsoft, das sind ja auch amerikanische Unternehmen und die bekommen ja eine Macht in diesem Sinne, weil sie diese Voreinstellung vornehmen und gegebenenfalls für ihre eigenen Produkte leichter unterlaufen können.

Florian Kugler: Ein Knackpunkt ist da ja fehlende Transparenz auf der einen Seite für den Nutzer, auf der anderen Seite fehlende Aufklärung …

Ilka Voss: … das ist es auch ja …

Florian Kugler: … und was auch immer mehr wird ist Smart Technology, die den Alltag wahrscheinlich in Zukunft noch stärker prägen wird als jetzt. Es ist wahrscheinlich nicht zu erwarten, aber es stellt sich die Frage, ob durch verstärkten Datenschutz es überhaupt zu erwarten ist, ob Nutzer in Zukunft überhaupt weniger digitale Spuren hinterlassen oder wird es weiter so exponentiell stark steigen, wie in den letzten Jahren?

Ilka Voss: Bei Smart Technology ist es auch noch einmal eine Frage, wie wird es denn da sein, wie ist denn da eine Grundeinstellung? Wenn ich Alexa nutze, was ist denn da die Grundeinstellung? Ich kann ja Alexa gar nicht nutzen ohne… als frage ich mich gerade. Wo ist der Grenzbereich? Wo funktionieren Produkte gar nicht mehr, wenn die Voreinstellung ist, ich kann nicht tracken? …

Florian Kugler: … Und wo kann man dort einen Opt-In geben gegebenenfalls. Es gibt ja auch die Smart-Buttons wo man direkt Produkte nachbestellen kann, bei Kaffeemaschinen oder Waschmaschinen. Wo wird da ein Opt-In eingeholt? Beim einmaligen Kauf oder bei jeder Transaktion, also das könnte ja kollidieren mit dem Gesetz gegebenenfalls.

Ilka Voss: Also ich finde, was bei dem Ganzen unterschätzt wird, ist die Aufklärungsarbeit auch, und ich glaube man hätte auch … Also was man im Markt sehr stark wahrnimmt, jetzt wird über die DSGVO sehr viel berichtet, und der Nutzer wird eigentlich aufgeklärt über die Medien aber es gibt keine Aufklärungskampagne in diesem Moment finde ich so richtig, und dass der Mehrwert dem Nutzer überhaupt bewusst gemacht wird. Jetzt habe ich das Gefühl, ist es mehr Aufwand für die Unternehmen, die betroffen sind, aber ich habe am wenigsten das Gefühl, dass die Nutzer jetzt sagen, endlich ist die DSGVO da, darauf habe ich lange gewartet, jetzt kann ich meinen Betroffenenrechten nachkommen. Wenn ich auch im Freundeskreis, im Privaten, gucken, dann ist es so, dass sie sagen, dass die DSGVO im Unternehmen eine Rolle spielt und, dass sie sich damit beschäftigen müssen, als dass sie sagen aus Nutzerperspektive, „oh ja endlich“, das sagt glaube ich gar keiner. Also ja die Datenschützer sagen endlich ist es soweit aber der normale Bürger, da würde ich eher nein sagen. Geht mir genauso, ich habe jetzt nicht drauf gewartet.

Florian Kugler: Also gestärkte Betroffenenrecht, aber zu träge User im Endeffekt. Das hatten wir ja bereits festgestellt, da würde sich eine Frage schlussendlich stellen, wie wird sich DSGVO bzw. auch die EPVO auf die User Experience auswirken?

Ilka Voss: Ja ich glaube das ist die Gradwanderung, dass ein Nutzer für sich wahrscheinlich später erkennen muss, die User Experience wird leiden, aus meiner Sicht, weil nach vorne hin, je mehr ich über den Nutzer weiß, und ich ihm gegebenenfalls personalisiert sein persönliches Nutzererlebnis zur Verfügung stellen kann, desto eher ist er ja zufrieden, und die Nutzer die das unterbinden, weil sie sagen, sie möchten ihre Daten nicht teilen oder ich möchte das eigentlich nicht, denen wird definitiv… also ist ja

ganz klar, ganz plakativ ist so ein Shop, also Otto jetzt, noch nicht mal gut personalisiert und dann habe ich das andere Produkt irgendwie, ich habe einer personalisierten Shop, der meine Voreinstellungen speichert, der genau weiß, was ich die letzten Male gekauft habe, was ich im Warenkorb hatte, ich kann meine Bestellungen mir angucken, die ich in der letzten Zeit getätigt habe, das hat ja sehr viel Convenience und erhöht die Nutzer Experience und das würde total verloren gehen aus meiner Sicht. Also das heißt, das ist ein Rückschritt und nur das dem Nutzer klar zu machen. Also vielleicht führt es dann dazu, dass man erstmal das Negativerlebnis gehabt und sagt, was ist denn das jetzt hier, jetzt finde ich mich ja gar nicht mehr zu recht auf so einer Plattform wie Otto, dann ändere ich das jetzt wieder, vielleicht muss es erst dazu kommen, dass der Nutzer erst den Mehrwert darin sieht, dass es auch ein Vorteil ist den Opt-In zu geben, um auf Basis von Daten und das müssen ja nicht mal die ganz spitzen Daten sein, es reichen ja auch schon so grundlegende Bewegungsdaten vom letzten Mal, dass es für mich einfacher ist mich zurechtzufinden, dass man mir meine (präferierten) Angebote unterbreitet.

Florian Kugler: Genau viele Geschäftsmodelle basieren ja auf einer datenbasierten Produktentwicklung, wurden immer optimiert durch Datenauswertungen. Insofern kann es wirklich große Konsequenzen geben für Geschäftsmodelle. Auf der anderen Seite der Werbemarkt ist ja auch für Otto interessant und da könnte es ja dahin gehen, wenn es keinen Opt-In gibt, dass keine personalisierte Werbung mehr ausgespielt werden kann, vielleicht erst im Zuge der EPVO aber da gibt es stimmen, dass erstmal deutlich mehr Werbung ausgespielt wird…

Ilka Voss: … ja also wieder breiter gestreut, also die Streuverluste die man früher hatte, nimmt man wieder in Kauf und das heißt es ist eher plakatieren, also wahllos Werbebotschaften raussenden, was auch aus Nutzer Sicht ein Nachteil ist. Also ich glaube es ist nicht wahrnehmbar, was da passiert ist, aber ich glaube schon, dass der Nutzer das negativ empfinden würde, wenn man den Schritt zurückgeht, so ein bisschen „back to the roots“, also wir hauen Kampagnen einfach breit raus, unabhängig davon wo der Nutzer ist und was wir von ihm wissen, also rein Umfeld getrieben, das es definitiv dazu führen wird, dass man mit deutlich mehr Werbung konfrontiert wird, die man nicht haben möchte.

Florian Kugler: Also könnte eine Entwicklung weg vom TKP hin zu mehr Klick-basierten Kostenstrukturen die Folge sein?

Ilka Voss: Das glaube ich gar nicht unbedingt. Also, dass mehr CPC-Modelle dahinter hängen?

Florian Kugler: Ja

Ilka Voss: Das geht sicher einher damit aber ich glaube nicht, dass es zwingend so ist. Das hätte ich gar nicht unbedingt angenommen.

Florian Kugler: Eine Frage stellt sich noch. Kann es sein, dass Nutzer und Konsumenten durch verstärkten Datenschutz einen höheren Wert für Unternehmen bekommen? Muss ein Unternehmen seine Bemühungen das perfekte Produkt noch mehr intensivieren obwohl den Unternehmen dann natürlich auch Schranken gesetzt werden, durch fehlende Personalisierung?

Ilka Voss: Das ist eine Hypothese, die kann man nachvollziehen. Also so mehr ich mein Produkt und ein Vorteil in Aussicht stelle, sobald er mir ein Opt-In gibt, weil er davon profitiert, ja klar, das erfordert von dem Unternehmen natürlich mehr in diese Richtung zu denken. Welche Kundenvorteile, auch wenn man das eigentlich nicht darf, welche Vorteile die ich einem Nutzer in Aussicht stellen kann und je mehr ich diese in Aussicht stellen kann, desto eher habe ich sein Opt-In, so löst es auf Unternehmensseite also den Druck aus, das Produkt noch mehr auf einzelne Kunden zuzuschneiden oder was kann ich in Aussicht stellen, also was du meintest, Vorteile in Aussicht zu stellen.

Florian Kugler: Also es könnte dazu führen, dass Unternehmen ihren Auftritt stark überdenken müssen und neue Wege finden müssen den Nutzer anzusprechen?

Ilka Voss: Ja also ich meine, wenn man jetzt mal das „worst-case Szenario“ sieht, morgen müssten wir einen Opt-IN haben und den haben wir jetzt nicht, dann setzt das auf jeden Fall auf Unternehmensseite andere Anforderungen voraus, also wenn ich sage ich habe keinen Opt-In mehr, dann sieht der Shop morgen ganz anders aus. Und dann trotzdem versucht man ja, das Produkt attraktiv zu gestalten, vielleicht einmal ohne Opt-In trotzdem, also darüber nachzudenken, aber gleichzeitig zu denken, was wäre mit dem Opt-In alles möglich und das in der Form als Produktentwicklung weiter nach vorne zu treiben. …

Florian Kugler: … und dann noch transparent darzustellen…

Ilka Voss: … Ja genau und das ist glaube ich die Herausforderung in der Kommunikation zum Nutzer hin zu sagen, gucke mal wenn uns das Opt-In gibst, dann sieht de Shop so aus und du hast viel mehr davon, aber das genau ist die Herausforderung.

X.II Experteninterview 2

Mi. 06.06.2018, 16:00 Uhr, Hamburg

Birgit Weyring

Teamleiterin Online Marketing • Affiliate Marketing

OTTO GmbH & CO. KG

Begrüßung des Interviewpartners, kurze Vorstellung der Master Thesis und Einholung einer Einwilligung zur Aufzeichnung und Veröffentlichung des Leitfadeninterviews.

Florian Kugler: Als ersten Punkt behandeln wir Datenschutz und die Relevanz der DSGVO. Die erste Frage wäre ob du die neue Gesetzgebung oder generell eine neue Gesetzgebung hinsichtlich Datenschutz für notwendig hältst?

Birgit Weyring: Ich könnte daraus die kürzeste aller Antworten machen und sagen ja. Selbst wenn ich da jetzt irgendwie immer so hin und hergerissen bin, weil ich beruflich sehe was für Möglichkeiten in dem Ganzen liegen. Ich glaube da bin ich schon überzeugt davon, du brauchst da Regelungen, du brauchst da Gesetzgebungen für. Vielleicht vorweggegriffen, ich weiß noch nicht genau ob unsere jetzige Lösung schon wirklich so das Non-Plus-Ultra ist. Manchmal ist man gezwungen sich weiterzuentwickeln, die Gesetzgebung kann da auch nicht stehen bleiben, aber ich halte es für richtig und wichtig, dass es ein Gesetz dazu gibt und das wir auch einen Datenschutz haben. Hier bin ich auch einfach sehr deutsch, so bin ich groß geworden, so bin ich sozialisiert.

Florian Kugler: Also eine Relevanz ist auf jeden Fall zu sehen und besonders in den heutigen Zeiten, es betrifft viele Bereiche jetzt nicht nur online Marktprozesse aber das ist natürlich auch ein Bereich, der davon betroffen ist bzw. Geschäftspraktiken und siehst du konkrete Auswirkungen der DSGVO auf Online Marketing Prozesse?

Birgit Weyring: Da ist glaube ich vieles so drin, wo es anfängt ein bisschen zu verschwimmen, weil wir in Deutschland diese Sonderlösung gebaut haben, die alte ePrivacy von 2003, das Telemediengesetzes was es gab und dann das alte Bundesdatenschutzgesetz, also der Vorgänger der ja auf deutscher Ebene war, die haben ja relativ viel schon geregelt und darum: manche Sachen haben sich da jetzt gar nicht so stark geändert, also es ist sehr viel mehr Administration dahin, weil du halt einfach Dinge dokumentieren musst ja und Dinge ändern musst im Zusammenspiel mit den Dreien, die ich genannt habe, die e-Privacy und dann würde ich sagen noch viel stärker was die neue machen wird und mit dem Telemediengesetz und wie ich die DSGVO auslege, kann das nämlich zu dieser Konsequenz kommen, ich habe entweder sehr große Veränderung oder nicht, also der deutsche Blick ist ja tendenziell immer noch drauf: ein Opt-In wird kommen die Frage ist wann und du kannst es nach heutiger Lage mit neuer Datenschutz Grundverordnung, altem Telemediengesetzes und noch alter e-Privacy so

auslegen, dass die deutschen Sonderlösung von du musst ein Opt-Out für diese klassischen Online Marketing Cookie Prozesse haben, dass das weiterhin gültig ist, dann würde ich sagen sind die Auswirkungen jetzt noch überschaubar, aber ich glaube sehr unterschiedlich für unterschiedliche Unternehmen abhängig davon wie groß man ist, wie viele Menschen man wirklich hat mit welchem Know-How die Online Marketing. Wenn ich das so sage, glaube ich die Punkte hast du auch noch mal und die sind auch immer noch hier die diskutierten, durch den vermehrten Aufwand den ich bezüglich Dokumentation habe oder ich muss mir Partner halt genauer angucken weil das ist ja einer der großen Punkte im Online Marketing, wo man auch heute schon sagen kann, egal ob es die e-Privacy gibt oder nicht, mit welchen Partnern arbeite ich zusammen und wie verarbeiten die Daten. Das ist wenn man ehrlich ist relativ aufwendig, das heißt wenn du dir diesen Luxus erlaubst, mit vielen Partnern zusammenarbeiten zu wollen und du gleichzeitig möglicherweise gar nicht so unendlich tiefes Know-How hast da zu hinterfragen was sie jetzt genau mit den Daten machen oder nicht, dann hast du schon eine sehr starke Änderung in den Marketing-Prozessen, weil du dann Entscheidung treffen musst in die Richtung von will ich vielleicht die Anzahl meiner Marketingpartner begrenzen, weil vorher habe ich das relativ entspannt gemacht und habe dann gesagt ja passt schon irgendwie, jetzt wo ich eigentlich in der Theorie nun mehr Organisation und mehr vertragliche Dinge habe, wie ich mache halt mit denen die AV, ich prüfe ob sie TOM´s, also die technischen und organisatorischen Maßnahmen getroffen habe, dass Zugriffsrechte und Benutzerrechte gegeben sind, kann man sich überlegen dass man Dinge einfach anders macht und dann würde es Marketing-Prozesse glaube ich schon sehr stark verändern, weil du dich dafür entscheidest, gewisse Sachen überhaupt nicht mehr zu tun, die du sonst einfach sehr gerne getestet hast, weil es irgendwie jetzt nicht so schwierig war, weil du einfach irgendeinen Partner oder Dienstleister hattest, der das gemacht hat und ehrlich gesagt war es kein riesen Thema. Wenn du heute das Risiko hast und unter Umständen eine Vertragsstrafe um die Ecke kommt, die dann am Ende doch, gerade als kleines Unternehmen, bei 20 Millionen sein könnte ich glaube realistisch gesehen immer noch nicht wahrscheinlich ist es ein kleines Unternehmen wenn es jetzt irgendwas mit dem Dienstleister gemacht hat was so nicht absehbar ist, direkt die 20.000.000 € bekommt aber als kleines Unternehmen können auch 150000 € schon weh tun oder selbst 50000 €.

Von daher, ich glaube das ist was los sein wird, bloß du hast im Markt gerade eine unheimliche Unsicherheit wie man überhaupt die ganze DSGVO lesen soll, also die ist ja hinlänglich unkonkret oder ich glaube für Juristen ist sie halt einfach ein typisches Gesetz, wo man sagen muss manche Dinge sind noch nicht wirklich entschieden und einfach nicht gerichtlich entschieden, wie man sie auslegen sollte. Das Gesetz erschafft eine Unsicherheitsphase und ich glaube abhängig davon wie viel Mut zum Risiko ein

Unternehmen hat, wird es halt auch irgendwelche Dinge anders machen oder nicht, also ein Unternehmen was sich die Zeit dafür nimmt und die Expertise hat seine Partner zu beleuchten, müsste die Prozesse nicht per se verändern. Ich glaube bei relativ vielen wird es das aber doch tun, weil es gewisse Konsequenzen in alle Richtungen hat.

Florian Kugler: Es hat sich ja nicht so viel geändert zum BDSG, Rechtsexperten sagen aber das viele Teile absoluter formuliert sind, also das Relativierung dann nicht mehr so leicht möglich sind und dazu kommen die und Bußgelder die anfallen also das ist vielleicht ein Druckmittel und wie du schon gesagt hast, Unternehmen trotzdem noch mal ihre Praktiken überdenken, also auf jeden Fall einen Anstoß gegeben ist. Sind denn Auswirkung durch e-Privacy des nächsten Jahres zu erwarten, betreffen die das Online-Marketing deutlich stärker?

Birgit Weyring: Ja würde ich auf jeden Fall so sehen. Weil gerade Deutschland ist eines der wenigen, vielleicht das einzige Land, dass sich die Möglichkeit zum Opt-Out herausgenommen hat und nicht damit bis heute schon gearbeitet hat. Sie sagen zur Verarbeitung der Daten und zur Marketing-seitigen Verarbeitung der Daten musst du ein explizites Opt-In des Nutzers haben. Deutschland ist eigentlich sehr weit schon mit einem Opt-In für die ganzen E-Mail Themen, die halt eben in den alten Gesetzen und Richtlinien verarbeitet waren, aber da braucht es eine neue Gesetzgebung wieder und du brauchst sie häufiger. Es passiert zu viel in dem Bereich und darum kannst du mit einem Gesetz was 10 oder 20 Jahre alt ist gar nicht alle heutigen Aspekte komplett damit abgreifen.
Und keiner kann in die Zukunft blicken um 20 Jahre vorher schon ein Gesetz zu machen was in 20 Jahren mit dem gewissen technologischen Fortschritt immer noch die Gültigkeit hat und wirklich alle Fälle abdeckt. Von daher ist es theoretisch nicht so viel anders aber praktisch hat es genau für das Online Thema ist es anders und die e-Privacy wird das halt einfach sehr stark ändern, weil dann nicht nur mehr die E-Mail geregelt ist die immer schon das Double-Opt-In, sogar in Deutschland, hatte, sondern dass halt jeder wirklich sagt, du brauchst ein sauberes Opt-In zur Verarbeitung der Daten. Der Prozentsatz ist klein. Wenige Menschen machen einen Opt-Out, bei einem Opt-In hingegen da gibt es ganz unterschiedliche Zahlen, welche Statistik man jetzt gerade nimmt oder welche Hochrechnung, ob es 10% der Menschen sind auf der Seite, die sagen ok ihr könnt meine Daten verarbeiten oder vielleicht doch 50 %. Ehrlich riesengroße Unsicherheit auf der Seite und wenn ich nur noch 10% der Daten als Basis habe, um gewisse Ableitungen zu treffen oder Analysen zu treffen macht das einen riesen Unterschied. Das heißt die e-Privacy wird die viel größere Auswirkung auf das Online-Marketing haben als die DSGVO hat.

Florian Kugler: Ein Opt-In wird dann wahrscheinlich verpflichtend sein, noch ist er es nicht zwingend...

Birgit Weyring: Es ist Lesart, es gibt den Düsseldorfer Kreis der Datenschützer. Die haben irgendwann einmal ausgelesen, dass man schon heute in dem Konstrukt so lesen muss, dass man das Opt-In eigentlich haben muss. Ist ein bisschen schwierig. Die DSGVO hat noch so einen Punkt, der sagt Interessenabwägung, dass du nach bestimmten Grundsätzen oder aber weil es noch vertretbar ist, was du möglicherweise an Daten sammelst, keinesfalls also was etwas sensibles angeht, die Ethnie oder was irgendwie deine Präferenzen sowohl irgendeiner Religionszugehörigkeit, deine sexuellen Orientierung und ich weiß jetzt nicht genau was alles die sensiblen Daten sind. Die sind im Online-Marketing nicht so relevant.

Florian Kugler: Ich habe es auch so rausgelesen, dass der Opt-Out heute nicht mehr die gängige Form sein darf.

Birgit Weyring: Ich glaube es ist eher noch die Frage wann müssen wir denn Opt-In machen und nicht mehr kommt er, sondern wann kommt er? Der Europäische Gerichtshof hat dazu eine Entscheidung bei sich liegen. Es gab früher scheinbar auch wirklich diese Aussage dass die deutsche Lesart mit dem Opt-Out in Ordnung ist auch in Brüssel. Es gibt heute scheinbar eher dann so dieses Verständnis, wir fanden das mal gut aber im Moment finden wir es eher nicht mehr gut. Und es wohl ein Verfahren vor dem Europäischen Gerichtshof ob das überhaupt in Ordnung ist. es ist nicht mehr wichtig Frage kommt ob, sondern wann wir einen Opt-In bekommen.

Florian Kugler: Google prescht ja bereits vor und auch andere Unternehmen holen bereits Opt-Ins ein. Wird der verstärkte Datenschutz sich auf die Marktmacht der großen Unternehmen wie Google und Facebook positiv auswirken oder eher negativ?

Birgit Weyring: Ich glaube das ist die große spannende Frage wo es wirklich hingehen wird. Die DSGVO in ihrer Reinkultur versucht sie glaube ich wirklich das zu erreichen, von sie wollen nicht die großen Stärken. In der Theorie könnte man da wirklich auslesen das wird gar nicht passieren, sie werden gleich behandelt, das ist so ein bisschen unterschiedlich und ich glaube da werden wir alle nicht wirklich den Blick haben, aber mit den Anstrengung die jetzt gerade auch ein Google unternimmt kann man schon jetzt mal hoffen, dass sie das Thema Datenschutz ernst nehmen, aber gefühlt immer mit so einem etwas schalen Beigeschmack weil es endet eigentlich immer damit, dass sie erstens Dinge machen die wirklich Datenschutz oder DSGVO relevant sein könnten, manchmal glaubt man haben sie genau die Lösung gefunden, die am Ende dafür gesorgt dass alle eigentlich noch stärker an sie gebunden werden. Häufig wird gesagt werden, wir können euch Daten nicht mehr geben, weil wir sind ja nicht so sicher sind, was ihr damit tut. Es ist schon besser wenn wir die Daten bei uns lassen und gebt uns doch einfach alle eure Daten und dann macht ihr die Attribution bei uns. Ist so ein Beispiel. Wo ich denke, netter Ansatz, DSGVO konform glaube ich und in der Theorie des Gesetzes super, die achten darauf, was sie mit ihren Daten machen. Für mich dann irgendwie der schale

Beigeschmack: ihr (Google) sagt jetzt: schwierig und bei den Partnern kann ich das nicht so richtig überblicken. Ihr verlangt von uns aber, das totale überzeugte: Alles gar kein Problem, ich schiebe alle unsere Daten zu euch Google, ihr seid der bessere Partner, finde ich persönlich schwierig und würde mich als Unternehmen schwer tun zu sagen ja klar ich schicke euch mal meine ganzen Daten rüber und dann macht ihr die Attribution für mich oder ich mache dir auf eurem System. Finde ich jetzt bisschen schwierig und darum befürchte ich ehrlich gesagt dass die Googles und Facebooks dieser Welt davon profitieren werden, weil dafür können sie nichts, da sie einfach ein ordentliches Produkt anbieten für den Nutzer. Denn wie du gesagt hast, dass sie sich jetzt einen Opt-In einholen. Also viele sagen ja sie ziehen die e-Privacy vor. Realistisch ist es eine Google Richtlinie die sie gerade in den Markt tragen und als Anbieter eines Produktes kannst du Richtlinien bestimmen nachdem du das Produkt nutzen kannst. Und dass die Richtlinie jetzt ungefähr dem auch entspricht was durch die e-Privacy zu erwarten wäre oder sie sind ja jetzt auch nicht böse und denken, oh deutscher Markt, wir wollen dir jetzt die e-Privacy vorab reindrücken und alle anderen europäischen Länder, ich glaube zumindest alle anderen, haben ja diesen Opt-Out nicht, sondern auch heute schon den Opt-In. Das heißt sie machen einfach eher nur eine Regel die für alle gilt. Wo Deutschland jetzt einfach nur einer von vielen ist, sie machen ja keine Sonderregelung für Deutschland, sondern eine generelle Regelung, alle anderen Ländern glauben, dass man einen Opt-In braucht. Sie schreiben nur in ihre Richtlinien für ihr Produkt, für ihr Programm, du musst dich an das halten, von dem wir bereits heute überzeugt sind, was in den meisten europäischen Ländern bereits gilt. Trotz einer manchmal kritischen Sicht auf Google, glaube ich nicht, dass sie da etwas Schlimmes tun. Wenn die Richtlinien für dich OK sind, dann nutz mein Produkt, wenn sie für dich nicht OK sind, dann nutze ein anderes Produkt. Ich befürchte aber eben dadurch, dass sie gute Produkte machen für den Endnutzer, dass alle sehr schnell an den Punkt kommen werden, dass wenn Google und Facebook auf den Opt-In gehen, dass sie diesen bekommen werden. Aus Nutzerperspektive gesehen. Während jedoch Tech-Anbieter XY ein viel größeres Problem haben wird und einfach nicht so viele Kunden haben wird, womit er sich Opt-Ins für seine Technologie holen kann oder womit seine Kunden sich Opt-Ins für Cookies oder sonstige Dinge holen können. Das heißt es ist nicht per se im Gesetz, dass sie bevorzugt werden, wenn man sich aber die Realität im Markt anguckt und wozu einfach dieses Gesetz vermutlich führen wird, ist die Lesart, dass sie ein Vorteil daraus haben. Ich glaube wahrscheinlich ist es eine Hypothese und es ist nichts was im Gesetz drin ist, aber ist die logische Konsequenz, wenn ich mir den Markt angucken, dass sie als der Gewinner des ganzen hervorgehen werden. Auch um den Punkt vom Anfang noch einmal aufzugreifen, wenn ich mich entscheide, ich möchte mit weniger Partnern testen und ich nehmen nur 2,3,4,5, dann ist die Wahrscheinlichkeit groß, dass Facebook und Google dabei ist und wenn ich

nicht gerade Retailer bin und OTTO heißte, dann ist die Wahrscheinlichkeit, dass wohl noch Amazon dabei ist, sehr hoch und das kann ich auch keinem verübeln. Also wenn du klein bist und eine überschaubare Ressourcenmenge hast oder irgendwie keine große BI hast oder selber nicht Daten arbeiten kannst, dann suchst du dir einen Partner der darin gut ist, das heißt der typischen Effekt einer der gut darin ist, kann durch gewisse Umstände einfach mal doppelt bevorzugt werden und ich glaube ehrlich gesagt, dass das passieren wird und das ist nichts was im Gesetz so drin ist oder was man per se sagen würde, die sind bevorzugt worden das sind sie nicht aber ich glaube durch die Randbedingungen wahrscheinlich das Ergebnis, dass sie da ganz positiv rauskommen werden und vielleicht auch einer der Gewinner sein werden auch wenn sie selber vielleicht sogar die sind, die die DSGVO sehr ernst nehmen.

Florian Kugler: Um zu konkretisieren, dass die DSGVO vielleicht auch den großen Playern in die Karten spielen könnte, sind die Punkte „Privacy by Design“ und „Privacy by Default“, die so als Verpflichtung ja auch neu sind und vorher noch nicht gesetzlich so aufgegriffen worden sind. Es ist zwar schon ein alter Diskussionspunkt, aber die sind jetzt auch gesetzlich inbegriffen. Wie bewertest du diese beiden Teile der DSGVO auch in Bezug vielleicht auf die großen Daten Raffinerien, weil diese ja auch eigene Browser anbieten, insofern auch die Möglichkeit haben, Gesetze so umzusetzen und auch vielleicht für Sie passend umzusetzen?

Birgit Weyring: Ich habe ja überzeugt gesagt, ich glaube wir brauchen Datenschutzgesetz, das ist meine Überzeugung, das könnte jetzt philosophisch werden, weil ich auch keine Lösung dafür habe, ist was wir haben wirklich gut? Ich glaube wirklich gut ist es nicht. Habe ich eine bessere Wahl? Weiß ich nicht. Irgendein kluger Mensch hat auch mal gemeint, dass die Demokratie gut ist, aber haben wir was Besseres? Also unsere Datenschutz Grundverordnung ist okay. Das Ziel zu sagen „Privacy by Design“ und „Privacy by Default“ klingt in der Theorie super, in der Praxis frage ich mich wirklich da aber auch, ist es überhaupt wirklich das was wir wollen, weil unter Umständen ist das auch nur Quatsch. Also wie der Nutzer heute agiert und irgendwie in Social-Media-Kanälen, in… ich weiß nicht ich will den Amazon Echo ins Haus oder ich stell mir einen Google Mini ins Haus und ich kann unter Umständen gute Dinge mit Profilierung und mit Modellen entwickeln. Bei Privacy by Design und Default kommt man ganz schnell auf diese Browser Diskussion, soll der Browser das schon irgendwie einbauen und das heißt, ich baue irgendwelche Dinge im Browser ein. Mal ehrlich gesagt die großen Browser dieser Welt kommen von Google, Microsoft und Apple und wenn man Facebook als App die sie sind sieht, und eine App ist ja de facto ein Browser bzw. ein eigenes Universum, de facto habe sie alle ihren eigenen Browser, können also ihre eigenen Regeln da machen. In der App mache ich sie nur für mein Universum, aber wenn Chrome der größte Browser ist und der gehört gleichzeitig demjenigen, der die meisten Daten in der westlichen Welt

hat. Und ich sage, wenn man dann ein Privacy by Design direkt in die Browser integrieren kann, dann wird es sehr schnell, sehr seltsam. Und was ist „Privacy by Design“ und „Privacy by Default“ eigentlich? Steht in der DSGVO drin minimale Datenhaltung? Ist es wirklich sinnvoll? Aber er ist wirklich gut, ist denn die Wahrheit? Es klingt wirklich super und im ersten Moment würde ich sagen, klasse, es gibt ja nichts Besseres. Will man das überhaupt? „Privacy by Design“ wird im schlimmsten Fall bedeuten, keiner kann sich mehr Login-Daten merken, keiner kann sich Cookies mehr merken, Cookies müsstest du sofort löschen, dein komplettes Browsen im Internet oder auf dem Smartphone wird deutlich weniger komfortabel sein und das wo Leuten mittlerweile wirklichen egal ist, wo ihre Daten landen. Natürlich möchte ich Nachhaltigkeit und ich möchte, dass jeder Arbeitnehmer auf dieser Welt von den Arbeitsbedingungen hat und in Wirklichkeit kauft jeder sein T-Shirt für 1,50 €. Iwo man weiß, da kann kein Arbeitsprozess hinter liegen, der wirklich vernünftig ist. Ich weiß nicht genau was du mit der Frage willst oder mit dem Punkt machen willst. Wie soll das funktionieren und funktioniert es dann wirklich so, wie es geplant ist und wenn wir dann jemand sagt: „Ja aber Google macht das doch total super in Chrome, dass du dich anmelden du kannst alles einstellen, ich sage nur wie schizophren ist das denn, ich muss mich bei Google, einem der Größten, bekannt machen damit ich da meine Vorlieben pflegen kann, damit ich anonym und mit Privatheit durchs Netz surfen kann, wenn ich eigentlich vorher vielleicht gar kein Google Konto habe, das ist doch schizophren.

Florian Kugler: In so einem Bereich wird eine Verpflichtung was „Privacy by Design“ und „Privacy by Default“ angeht problematisch. Wir können ja mal zur Nutzerperspektive kommen was man sich mal vorstellen könnte, ist der Fall, dass ein Opt-In oder Opt-Out eine Grundeinstellung wäre. Hier stellt sich die Frage ob die DSGVO, wenn Sie das voraussetzt, was sie erreichen will, die Stärkung der Betroffenenrechte, um dem User mehr Selbstbestimmung zu geben im Netz, das ist ja das Ziel. Gibt man dem Nutzer also wirklich mehr Selbstbestimmung, wenn es eine Voreinstellung mit dem Zweck der Datenminimierung gibt ist die Frage: Glaubst du, dass Nutzer in Zukunft den Opt-In verweigern werden oder im großen Maße dann doch tätigen werden?

Birgit Weyring: Ich glaube und das ist eine meiner ganz wenigen Überzeugung an die Bequemlichkeit des Nutzers, wer auch immer es schaffen wird, so viel mehr Bequemlichkeit für den Nutzer zu schaffen, dass der Nutzer willens ist dafür einen Opt-In zu geben, wird Opt-Ins in hohem Maße kriegen und ich glaube auch wirklich, dass Bequemlichkeit da der wichtige Punkte ist und da geht's dann glaube ich nicht mehr darum wer hat noch welche Daten von mir und wie viele Daten von mir. Die berühmte Startup Mentalität, wenn das Produkt gut genug ist interessiert dich eigentlich nicht mehr was da irgendwo im Hintergrund passiert. Ich glaube generell wird es immer schwieriger werden. Ich glaube nicht, dass auch nur ansatzweise die Mehrheit der Nutzer versteht was da

wirklich passiert und was mit Daten möglich ist und was die Konsequenzen von Dingen sind, die sie tun und wenn wir dann an solchen Punkten sind, Dinge sollen einfacher werden, aber z.B. Datenschutzerklärungen sind deutlich länger geworden. Ich glaube der Anteil derjenigen die das komplett lesen, wird deutlich kleiner werden und dann hat das Gesetz glaube ich nicht wirklich erreicht was es wollte. Unternehmen versuchen es transparenter zu machen, beim Nutzer wird nicht ankommen. Darum, ich glaube der Nutzer wird in der Theorie da auch immer sagen, ja ich kauf halt auch nur nachhaltig und natürlich möchte ich nur Fleisch aus Biohaltung und alles andere ist schlecht. In einer Umfrage würde jeder Nutzer immer sagen, Datenschutz ist total wichtig, in der Praxis glaube ich wirklich mit einem Angebot, das überzeugend ist, interessiert keine Menschenseele. Im Zweifel werden sie ihre Seele dafür verkaufen als Nutzer. Nicht böse gemeint, nicht als Vorwurf, sondern als realistische Betrachtung. Das hast du ja heute schon auf einer Cookie Ebene, im Ernst lösche deine Cookies und bei allen die nicht wirklich irgendwelche anderen hochaufwendigen technischen Verfahren machen, die ich im Zweifelsfall auch einfach hätte verbieten können, könntest du heute ja schon ganz gut hinkriegen, dass du einfach so zu sagen immer mal wieder deine Datenströme kappen kannst.

Ich glaube die DSGVO hat der Sache an der Stelle auch ganz ehrlich gesagt ein Bärendienst erwiesen, weil alle sehr kreativ da drin sind innerhalb der gesetzlichen Möglichkeiten jetzt Mittel und Wege zu finden, wie ich eine viel nachhaltigere Datenwegschreibung hinbekomme und ich glaube innerhalb der gesetzlichen Möglichkeiten gibt es da jetzt viel mehr, als wir dumm auf Cookies gearbeitet haben, viel einfacher eigentlich die die Spuren irgendwie zu verwischen oder irgendwie zu kappen und ich glaube das wird schwieriger und ich glaube trotzdem, dass weniger die Masse der Seiten weniger Opt-Ins kriegen.

Florian Kugler: Datensparsamkeit dann auch die ganzen gestärkten Betroffenenrechte, wie das Recht auf Löschung, das Recht auf Datenportabilität, Informationspflichten, Auskunftspflichten, das sind ja alles Bereiche die deutlich gestärkt wurden. Glaubst du denn das Nutzer diese Rechte wahrnehmen werden oder werden sie ihre Selbstbestimmung im Netz doch weiterhin lieber für irgendwelche Vorteile oder die Nutzung von Produkten und auch sehr leicht aufgeben?

Birgit Weyring: Ich bin da sehr zynisch. Ich glaube, dass die Bequemlichkeit siegen wird. Wenn das jemand für sich entscheidet, egal wie bewusst oder unbewusst deine Entscheidung ist, stoppe mich, aber es ist die Entscheidung eines jeden Einzelnen. Ich könnte es auch wieder zynisch sagen und etwas überspitzt, ich glaube schon, dass es diverse Rentner im Ruhestand gibt, die mit einer großen Begeisterung überall sich jetzt die Informationen zu Ihrem Konten geben lassen die auch immer mal wieder gerne irgendwelche Löschaufträge geben und ich glaube das ist ja auch alles vernünftig. Also

es wird sicherlich eine Zielgruppe geben für die die DSGVO genau richtig ist, die werden all die Möglichkeiten, die sie ihnen jetzt bietet und die einfach positiv an dieser Stelle für die Menschen sind, nutzen, werden sagen okay das mache ich und für die ist es gut. Ich glaube es gibt die Mehrheit von Menschen, die sich Auskunft geben lassen und ab und an darum bitten, dass Daten gelöscht werden. Ich glaube auch für die ist es grundsätzlich gut, ich bin mir aber nicht ganz sicher ob sie wirklich die Mehrheit sind. Es wird mindestens eine kleine Minderheit und Umstellung auf ihre große, vielleicht auch die Mehrheit geben, die ehrlich sagen, es ist jetzt schön, dass ich das habe aber ehrlich gesagt ich glaube nicht, dass das besonders viele Menschen nutzen werden. Ist aber eine reine Hypothese, wo ich sagen würde es könnte 50/50 sein. Es ist schön, dass man die Möglichkeit hat, ich bezweifle bisschen daran, dass jemand sich diesen Aufwand machen wird. Da ist es auch die Schwierigkeit, wenn wir jetzt über Online Marketing reden, und Profilierung und Scorings, was will ich denn in einer Beauskunftung als Information bekommen, was irgendwie relevant ist, also das ist jetzt sehr stark Online Marketing bezogen. Also es ist sehr spannend zu wissen, wer hat noch keine Kontendaten und zu irgendjemanden, einem Online Retailer, wo du sagst ich bestell bei dem Nichts mehr, lösche mein Kundenkonto und du weißt es jetzt sicher, du kannst dir vorher die Informationen geben lassen danach wird es gelöscht und gut. Lohnt sich dafür der ganze Aufwand, ich weiß nicht. Und wenn es doch einige machen, dann ist es für die eine gute Basis, und vielleicht liege ich auch falsch und es gibt eine große Anzahl Menschen, die das machen und genau darauf gewartet haben. Dann ist es ja auch schön.

Florian Kugler: Selbst, wenn die Verordnung nochmal als Appell an die Unternehmen dient, auch wirklich die Sachen einzuhalten, die auch schon vorher vorgeschrieben waren oder wichtig waren, auch eine Blaupause für die Zukunft zu bieten. Jetzt noch mal eine andere Perspektive, neben Betroffenenrechten geht es ja auch um die Convenience im Netz und um User Experience und es wäre ja auch in heutigen Zeiten eigentlich nicht wünschenswert wenn User Experience negativ beeinflusst wird, wird die DSGVO und dann speziell vielleicht e-Privacy-verordnung, wenn die dann das Opt-In wirklich vorschreibt, die User Experience beeinflussen?

Birgit Weyring: Ich fürchte ehrlich gesagt sagen, ja. Denn ich finde allein schon, dass du bewusst überall die Abfrage bekommen wirst, dürfen wir deine Daten speichern. Das ist einfach ein Unterschied. Also das gibt's heute schon auf vielen Seiten, ja diesen grässlichen Cookie Banner. Aber der hat bis jetzt ja relativ wenig Konsequenz und den kann ich relativ einfach wegklicken. Aber wenn man jetzt das ernst nehmen würde und sagen würde der ist nicht nur eine Alibifunktion, die da irgendwo im Browser ist und ich versuche wirklich den Nutzer sinnvoll zu informieren und eine gewisse Transparenz darüber zu geben was passiert, was ja eigentlich die Idee dahinter ist, dann hat er glaube ich eher einen etwas nervigen Effekt. Wenn man die DSGVO eigentlich mal sehr hart

sieht, müsste man im schlimmsten Fall ja davon ausgehen, geht sie ja irgendwie mit Privacy by Design und Default davon aus etwas wegzuschreiben, was für den Nutzer eigentlich von der Experience viel besser ist. Ich habe dich in einem Browser erkannt, ich erkenne dich in einem anderen wieder. Ich zeige dir einfach diese Cookie Banner Einstellungen nicht mehr, sondern ich unterstelle einfach mal, wenn du irgendwo eine gewisse Freigabe für gewisse Dinge gegeben hast, dann ist das hoffentlich so, dass du sie mir gegeben hast und nicht nur irgendwie einen bestimmten Gerät, das also für dich derselbe Wunsch ist, dass die selben Regeln für deinen Desktop im Büro gelten, wie für dein Smartphone zuhause. Da fängt man an eigentlich schon vorsichtig zu werden, weil wenn ich das tue kann ich es wirklich etwas angenehmer machen für den Nutzer, ich schreibe also gewisse Informationen am Nutzer weg und kann die überall wiederverwenden. Ist das dann noch Privacy by Design und Default oder ist es nicht wieder, ich profiliere wieder oder schreibe mehr Informationen weg als ich jetzt zwingend nötig brauche, also es ist bequemer für den Nutzer und positiver für den Nutzer und die Experience wird dadurch besser werden, aber kann ich das noch als Interessensabwägung machen oder nicht, oder muss ich korrekter Weise immer fragen, ob er sein Einverständnis überall gibt. Oder zweite Möglichkeit, ich versuche die Login-Quote überall zu erhöhen, weil ich mir damit die Informationen sauberer wegschreiben kann, aber ist es von der User-Experience besser, wenn ich jetzt permanent überall gefragt werde, ob ich mich einloggen möchte. Ich darf ja keine Cookie Wall machen, ich muss das Angebot ja trotzdem zugänglich machen, egal ob er einstimmt oder nicht oder sich einloggt oder nicht. Ich glaube die Nutzerbedürfnisse sind so unterschiedlich, dass ein Gesetz es schaffen würde die User Experience jetzt nachhaltig zu verbessern.

Florian Kugler: Ich glaube die Diskussion anzufangen, ob Personalisierung gleich Steuerung ist, greift deutlich zu weit. Aber das ist ja gerade ein interessanter Bereich, viele User nehmen personalisierte Websites, speziell im e-Commerce, als Mehrwert wahr. Besonders wenn man auf so großen Plattformen unterwegs ist wie OTTO, dann freut man sich schon die Produkte angezeigt zu bekommen die einen interessieren und es hilft ja auch sich zurecht zu finden. Wenn man sich an einer Privacy by Default oder Design Einstellung bei der Erstellung einer Website orientiert, dann würde man ja eher eine nicht personalisierte Website bauen. Da stellt sich die Frage was besser ist für den User, das ist natürlich auch eine ethische Frage, es wird sich auf die heutige User Experience dann doch schon negativ auswirken?

Birgit Weyring: Das würde ich auch befürchten. Wobei vielleicht das ist ja das Gute, das Positive daran. Unter Umständen erkennt dann jede gute Möglichkeit, wie man Dinge wirklich besser machen kann und wie man es rechtskonform macht, ich glaube in jedem Wandel steckt auch eine Chance, wo kann ich denn Dinge verbessern oder sauberer machen. Vielleicht kommt es auch anders und das keine seinen Opt-In gibt ist

totaler Quatsch und es wird eher dazu kommen, dass es vielleicht ein kleinerer Teil derjenigen sein wird, die einen Opt-In setzen aber das sind diejenigen, die es wirklich zu schätzen wissen. Und das heißt, ich habe eine deutlich sauberere Trennung, wer möchte eigentlich Personalisierung und wer kriegt die, und wer muss dann damit leben, dass er es mit der Schrotflinte kriegt, weil Werbung kriegt man ja trotzdem. Das ist ja eine Illusion derer sich viel hingeben, ich kriege dann keine Werbung mehr. Das ist ja Quatsch. Und manchmal mag Streuverlust ja auch positiv sein. Ich glaube auch darin liegt auch eine Chance und User Experience wird noch ein super spannendes Thema dabei werden. Und jeder ist gut darin beraten zu erkennen, was will der Nutzer da wirklich. Es kann also ein Differenzierungsmerkmal sein in der Umsetzung dieser Richtlinie und dieses Gesetzes.

X.III Experteninterview 3

Mo. 09.07.2018, 13:00 Uhr, Hamburg

Björn Stecher

Stellvertretender Vorsitzender der D21 Initiative e.V.

Begrüßung des Interviewpartners, kurze Vorstellung der Master Thesis und Einholung einer Einwilligung zur Aufzeichnung und Veröffentlichung des Leitfadeninterviews.

Florian Kugler: Intro kurze Vorstellung der Master Thesis

Björn Stecher: Ganz interessant ist der Punkt, dass Transparenz nicht gleich mehr Selbstbestimmtheit zur Folge hat. Je mehr Transparenz, ein ganz interessantes Phänomen bei der DSGVO, da sie ja auf mehr Transparenz baut, sie aber nicht zwangsläufig dazu führen muss, dass man selbstbestimmter agiert. Hintergrund ist der, dass man mit so viele Informationen zugespielt werden kann, wenn ich nicht die notwendige Kompetenz habe, sie einzuordnen, oder ein Recht auf Einfachheit habe, mir über die Auswirkungen, gar nicht mehr bewusst sein kann, und ich dann auch im Netz nur eine Scheinselbstbestimmtheit habe. Die Frage ist, wie kann man die Balance zwischen mehr Transparenz und mehr Information, und Informations-Overflow, wie kann man die austarieren, um dann wirklich den Grad der Selbstbestimmtheit dann zu messen. Das ist ein recht interessanter und wichtiger Punkt, dass man nicht nach mehr Transparenz schreien kann: Ich glaube wir haben in vielen Bereichen bereits ein sehr hohes Maß an Transparenz. Aber wir sehen auch an dem Datenschutz Paradoxon, dass mehr Transparenz und mehr Informationen nicht zwangsläufig dazu führen, dass der Nutzer sich selbstbestimmter im Bereich Datenschutz bewegt.

Florian Kugler: Wir können jetzt gerne zu den Fragen überleiten. Vielleicht geben Sie zunächst einen Einblick, was ihre Expertise betrifft auf diesem Gebiet.

Björn Stecher: Ich selber bin von Haus aus Jurist und zertifizierter Datenschutzbeauftragter im Bereich der DSGVO und auch im Rahmen der D21, wo ich mehrere Hüte aufhabe und auch im Beratungstechnischen Kontext aktiv bin, viele Startups berate und auch größere Unternehmen in der Umsetzung von Datenschutzrichtlinien und Datenschutzbestimmungen. Auch versuche ich im Rahmen der D21 Initiative die Nutzer im Bereich des Paradoxons was sie angesprochen haben, aufzuklären, und versuchen auch mit innovativen Methoden, Datenschutz neu zu denke und das mit verschiedenen Akteuren und Stakeholdern zu diskutieren. Ich spreche immer ganz gerne von Datensouveränität und Datenbestimmtheit, wie kann man Leute dazu befähigen, sich in der digitalen Welt, kompetenter zu bewegen. Damit hat man natürlich im operativen wie im politischen Bereich, den Versuch den innovativen Ansatz auch hier fahren zu können,

der Bereich auch zu verändern und einen Blick auf die DSGVO zu haben. Das zur Einordnung.

Florian Kugler: Ja vielen Dank, das passt auch sehr gut. Ich habe bisher auch verschiedene Datenschutzexperten oder -koordinatoren in Unternehmen, sehr stark auch mit dem Online-Marketing Fokus, befragt. Insofern ist das eine sehr gute Ergänzung und bringt noch einmal eine neue Perspektive in meine Arbeit. Dann würde ich direkt mit der ersten Frage starten. Halten Sie eine neue Gesetzgebung hinsichtlich Datenschutz für notwendig?

Björn Stecher: In diesem Fall die DSGVO?

Florian Kugler: Ja es gab ja bereits einige Vorgänger. In diesem Fall zur DSGVO, ist es wichtig hier so ein Update zu haben?

Björn Stecher: Ja, brauchen wir. Das wird die spannende Frage sein, denn die DSGVO hat jetzt schon Bestandteile, die auf bestimmte Zukunftsszenarien keine Antwort hat, die nach ihr auch nicht geregelt werden können. Zum Beispiel, man hat immer noch das Problem, dass man Daten, oder Personenbezogenheit definieren muss, nach der das Datenschutzgesetz dann auch gilt. Die aber perspektivisch dahinkommen werden, dass bei den meisten Daten, die zur Verfügung stehen, immer irgendwo einen Personenbezug hergestellt werden kann. Da ist die Frage ob man diese Trennung zwischen Personenbezug überhaupt in Zukunft noch haben muss, oder ob man generell so ein Datenrecht machen sollte. Das ist das Eine, das Zweite ist, dass wir immer noch ein Problem damit haben, dass selbst bei Datenkategorien, die einen geringen Sicherheitsstandard haben, bei der Leute sehr inflationär damit umgehen, bspw. Mit der eigenen Email-Adresse, die aber den gleichen Schutzstandard haben wie meine Bewegungsprofile. Das heißt es ist notwendig Datenschutz aufzubrechen und zu clustern, nach bestimmten Datensicherheitsniveaus. Jetzt mal sehr pauschal gemacht, nach sensiblen Daten und nach nicht-sensiblen Daten, die einen besonderen Schutz bedürfen. Aber ich glaube wir können hier kleinteiliger arbeiten. Das heißt mit meiner Email-Adresse kann ich anders umgehen als mit meinem Bewegungsprofil, mit meinen Bewegungsdaten gehe ich anders um, als mit meinen Online-Daten, mit meinen Einkaufsdaten gehe ich anders um als mit meinen medizinischen Daten. Und diese Kategorien, wenn man mit so einem Kaskadenmodell arbeiten würde, und dass auch gesetzlich umsetzen kann, dann könnte man immer eine andere Rechtskonsequenz daran anschließen. Da würde die Gesetzgebung etwas aufweichen. Und dieses Kaskadenmodell hat die Folge, dass Leute in ihrem subjektiven Datenschutz besser abgeholt werden. Also subjektiver Datenschutz bedeutet, dass ich mit meinen Daten anders umgehe, also sie verteufeln z.B. Facebook, ich nicht, sie verteufeln nicht Twitter, ich verteufele Twitter. Sie gehen Online einkaufen, ich nicht. Die Subjektivität des eigenen Datenschutzbewusstseins ist viel essenzieller und muss sich auch in Gesetzgebung wiederfinden. Mehr als dieses pauschale, das ist

alles in Datenschutz mit drin und ich muss immer für alles einwilligen, und das nervt für die User, die sehr offen sind, bewusst offen sind, im Umgang mit ihren Daten, nervt das. Das brauchen wir nicht. Diese Varianz muss sich auch zunehmend in der Gesetzgebung abbilden. Der letzte Punkt: auch die DSGVO krankt an einem wesentlichen Element, und da müssen neue Instrumentarien her, und das ist das Instrument der Einwilligung. Es ist wichtig und richtig wie es ist, krankt aber daran der Datenschutz. Weil meine These ist, je mehr ich einwilligen muss in einem sehr komplexen Sachverhalt, in einer unheimlich komplexen Materie, die multidimensional ist, ich eigentlich über die Folgen und Konsequenzen gar nicht mehr kritisch reflektieren kann, gar nicht mehr abwägen kann. Die Einwilligung eigentlich ad Absurdum führt. Wenn ich über die Ampel gehe und die Ampel ist rot, dann weiß ich, ich kann ich sterben. Wenn ich jetzt dem und dem den Datensatz zur Verfügung stelle, weiß ich jetzt nicht, ob das für mich wirklich so schädlich ist, ob man mich mit diesen Daten in Kombination mit anderen wirklich ausspionieren kann, oder ob sie wirklich dazu da sind durch mein User Verhalten die Website zu verbessern, ich hab so mannigfaltig komplexe Sachverhalte, ich habe keine klare User-Wirkungskette, deswegen kann ich auch nicht wirklich eine klare informierte Einwilligung abgeben. Und hier brauchen wir neue Instrumentarien, die müssen anders funktionieren. Weil sonst wird immer die Hauptverantwortung auf die Verbraucher, auf die Endnutzer abgeschoben und auch die DSGVO macht das. Das ist das einzige. Verfügbare Mittel, dass wir haben, ich versteh das, besser als gar keins. Aber wenn wir über eine neue Gesetzgebung reden, dann muss dieses Instrument der Einwilligung durch ein neues sinnvolles Instrument ersetzt werden. Nicht um weniger Datenschutz aber es muss ersetzt werden.

Florian Kugler: Ja ich denke auch, wenn man ein Ja oder Nein beim Aufruf einer Website abgibt, tut man das auch abhängig von einer flüssigen User-Experience sehr schnell und ohne hinter die Kulissen zu schauen. Was natürlich interessant ist, was sie auch angesprochen haben gerade, ist, dass es verschieden Bereiche gibt, die eine unterschiedliche Behandlung bedürfen und dass man das auch trennen muss, also nicht ein Datenschutzgesetz für alle Anwendungen, sondern auch auf kleinere Bereiche bezogen. Sehen Sie denn in der DSGVO auch speziell Online-Marketing-Prozesse behandelt? Welche Auswirkungen sehen Sie hier also speziell auf das Online Marketing, auf Prozesse wie Tracking oder Profiling? Greift das hier weit genug, ist die Anwendbarkeit hier gegeben? Sind hier also klare Auswirkungen zu erwarten?

Björn Stecher: Ja es wird Konsequenzen geben. Profiling ist natürlich sehr stark enthalten, und hat auch unternehmerisch Konsequenzen in der Umsetzung und Erstellung von Datensicherheit. Insofern die DSGVO ganz klar Einfluss haben auf Marketing-Prozesse. Sowohl was das Targeting an sich angeht, das ist notwendig, also für Datenschutzfolgeabschätzungen, die zwingend notwendig sind, wenn ich im Bereich Profiling bin, wenn ich Daten zusammenbringe, dass ich das dann offenlegen muss, das ist das

eine. Zum anderen ist wichtig, dass ich deutlich mache, wie ich mit Themen wie Privacy by Design und Default umgehe. Da muss ich meine Kommunikationsmaßnahmen natürlich auch intensiver bewerten, und die Umsetzungen dann auch wirklich transparent machen, wie ich bei einem bestimmten Prozess, bei einer bestimmten Dienstleistung, einem bestimmten Produkt, nach diesen Kriterien entwickelt habe. Dann wird die DSGVO in der Gänze auf jeden Fall Auswirkungen auf Online Marketing Prozesse haben. Und das Online Marketing in der Außendarstellung festgehalten, einen Spagat führen muss, weil die DSGVO sagt, die Erklärungen zum Datenschutz müssen einfach sein. Müssen aber auch informierter sein. Dann muss Nutzer aber auch in einer umfassenden Transparenz gewährleistet werden. Es ist notwendig die Bestimmungen immer auf die jeweiligen Rechtsgrundlagen abzustellen. Da sind so viel in sich wiederkehrende Zielkonflikte enthalten und den Spagat musst du im Online Marketing auch irgendwie schaffen. Ich muss ja darüber informieren, wenn ich jemanden als User tracken will, da habe ich die Verantwortung. Wie kann ich jemanden dazu bringen, dass er mir seine Daten zur Verfügung stellt? Das muss ich einfach und klar machen und das beißt sich aber schon, wenn die Anforderungen der DSGVO dahingehen, ich muss immer sehr informiert sein. Das wird sehr schwer, sehr spannend sein.

Florian Kugler: Ich denke auch, besonders wenn es in die Richtung geht, dass immer ein beschreibendes Opt-In nötig ist, wenn man eine Seite aufruft, weil da programmatisch ausgesteuerte Banner hinterlegt sind. Das wäre ja für die UX sehr kritisch. Was ja in der DSGVO auch immer thematisiert wird, sind erwartbare Maßnahmen, das ist natürlich auch ein sehr schwammiger Begriff. Und hier stellt man sich in der Branche die Frage wie Maßnahmen wie Retargeting behandelt werden, das ist ja vielleicht eine erwartbare Maßnahme. Wie stehen sie dazu?

Björn Stecher: Zum Retargeting?

Florian Kugler: Ja.

Björn Stecher: Naja, wenn es den Voraussetzungen der DSGVO entspricht ist es natürlich auch legitim. Die Frage ist, ob der Nutzer die notwendige Kompetenz hat, zu wissen was Retargeting ist und welcher Vorteil sich dadurch bietet.

Florian Kugler: Um vorweg zu greifen. Die DSGVO wird ja noch einmal durch eine neue ePrivacy-Richtlinie ergänzt. Welche Unterschiede im Bereich der Auswirkungen sind hier zu erwarten? Wird es nochmal deutlich schärfer? Und wann ist überhaupt mit der EPVO zu rechnen?

Björn Stecher: Die EPVO sollte eigentlich zum Start der DSGVO da sein, ist sie nicht. Geplant nach meinem letzten Stand, Herbst nächsten Jahres (2019). Inwiefern die EPVO noch einmal schärfere Maßnahmen oder eine Konkretisierung beinhaltet, sei ja auch noch einmal dahingestellt. Sie wird sehr stark lobbyiert von den Online Marketeers. Da müssen wir schauen, ob sie Prozesse wie Retargeting schärfer behandelt. Ist ein

Blick in die Glaskugle, kann man erstmal nicht wissen. Es ist rein rechtsdogmatisch ob sie zur DSGVO eine Konkretisierung ist, insofern mag ich da gerade auch keine Prognose abgeben. Also Anfang des Jahres war das Geschrei über die Erwartungen zu EPVO sehr groß, dann haben sich die Juristen rauf gestürzt, eigentlich müsste die EPVO in die DSGVO mit eingebettet werden. Dann sind alle Stimmen erstmal ruhig geworden. Insofern mag ich da jetzt tauch keine Prognose abgeben.

Florian Kugler: Okay. Sehr interessant für die Arbeit ist auch die Rolle, die die großen Unternehmen auf dem Markt spielen. Speziell Google und Facebook. Google dominiert ja einige Bereiche des Online Marketings mit einem Marktanteil von beinahe 90%. Hier ist die Frage, wie wirkt sich die DSGVO positiv oder negativ auf die Marktmacht der großen Unternehmen auf dem Werbemarkt wie Google oder Facebook aus? Haben sie es vielleicht leichter so etwas umzusetzen?

Björn Stecher: Also wenn Sie jetzt die finanziellen Auswirkungen für Google und Facebook betrachten, dann wohl eher negativ. Wenn sie die Auswirkungen auf die Realisierung der Umsetzungen sehen, dann werden diese Unternehmen gerade diejenigen sein, die es umsetzen können. Oder, die den Anschein erregen könnten, dass es umgesetzt wird. Deswegen wird sich die DSGVO auch nicht negativ auf die Marktmacht der großen Unternehmen auswirken, das glaube ich in keiner Weise. Weil diese Unternehmen die notwendigen Realisierungselemente haben, um die DSGVO so umzusetzen, dass sich das Geschäftsfeld auch dort wiederfindet. Es hat eher Auswirkungen auf mittelständische Unternehmen. Die ganz intensiv mit den Plattformmodellen arbeiten. Facebook versucht ja gerade die ersten Maßnahmen umzusetzen. Die Marktmacht könnte dann eingeschränkt werden, wenn ich überprüfe ob bei Google oder Facebook die Regelungen der DSGVO nicht umgesetzt werden können. Dafür brauchen Sie jemanden, der die Kompetenz hat, in dem jeweiligen Unternehmen, die Datenschutzprozesse vollumfassend zu bewerten, da brauchen sie jemanden der die Komplexität dieser großen Konzerne verstehen und begreifen kann und in datenschutzrechtlichen Belange auch umsetzen kann, und das ist fast schier unmöglich. Das ist meine These. Allein herauszufinden, ob es datenschutzrechtlich relevant ist, wie funktioniert der Algorithmus von Facebook, nach welchen Kriterien. Wie kann ich, wenn ich bestimmte Kriterien nicht mehr zu Verfügung stelle, wie wirkt sich das wirklich aus? Wie ist es wenn anonymisierte Daten von Facebook benutzt werden, dann findet die DSGVO ja keine Anwendung. Wenn das passiert, wie hoch ist der Aufwand die Daten wieder zu deanalysieren. Ist Facebook dazu in Der Lage? Allein diese Detailfragen haben schon eine enorm hohe Komplexität, dass es schier unmöglich ist, in all seiner Gänze so zu überprüfen. Das kann nur das Unternehmen aus sich heraus machen. Und da rede ich nicht nur von dem was der Nutzer letztendlich sieht, sondern von dem was letztendlich tatsächlich möglich ist. Oder welche Daten auch an Dritte weitergeleitet werden. Das ist ja dieser große Aufschrei mit

Cambridge Analytica. Wo Facebook selber nicht mehr weiß, welche Daten, Dritten zugänglich gemacht worden sind. Da kann man nur mit Pauschalitäten arbeiten. Will heißen in der Summe, nein die Marktmacht wird nicht negativ beeinflusst auf die Unternehmen mit de DSGVO. Rein Marketing-technisch von den großen aber positiv ausgelegt werden und zur Stabilisierung der Marktmacht der großen führen.

Florian Kugler: Hier ist ein sehr interessanter Faktor, dass man auf den großen Plattformen, in den großen Ökosystemen eingeloggt ist und bleibt, und darüber hinaus ja auch einige Verfügungsrechte abgibt. Greift bei so welchen Ökosystemen das Kopplungsverbot noch? Ist es rechtens, dass man mit zielgruppenbasierter, ausgesteuerter Werbung bespielt wird innerhalb eines Ökosystems, nur weil man eingeloggt ist?

Björn Stecher: Das wird nicht greifen. Sie haben recht mit dem Kopplungsverbot, aber es wird nicht greifen. Sonst könnte man ja komplette Geschäftsmodelle damit kaputtmachen, wie von Facebook. Wenn das Kopplungsverbot soweit greifen würde, dann würde man das Ganze ja ad Absurdum führe. Was sie brauchen in dem Kontext ist, dass sie nicht eine sanktionierbare Regel gemäß DSGVO haben, sie müssen das Unternehmen in ihrer Anbindung, in ihrer Logik und ihrer Auswirkung müssen sie reglementieren. Da können sie in Debatten machen wie dem Daten-Ethik-Code, dass sich jedes Unternehmen eine Corporate Digital Responsibility auferlegt. Dass diese Code of Conduct in der Verwendung von Daten rechtlich zwar sauber ist, oder zum Teil als Black Box nicht mehr kontrollierbar ist, die Auswirkung, die mit der Verwendung der Daten eihergeht, dass die sanktionierbar sind. IBM hat ja vor einiger Zeit den Terrorist Score entwickelt, dieser Terrorist Score belegt Personen mit einem Score, der die Wahrscheinlichkeit angibt, ob sie ein Terrorist sind. Was IBM gemacht hat, sie haben sich nur von Daten bedient, die von Twitter zur Verfügung gestellt worden sind. Das heißt sie haben nur rechtlich zugängliche Daten, da darf keiner was sagen, es bedarf keiner Einwilligung, alles war sauber. Alles ist DSGVO rechtlich konform. Die Verwendung hat aber eine ethische Komponente, da es gesellschaftlich nicht akzeptiert wird, denn niemand sollte mit einem Terrorist Score rumlaufen müssen und sich dafür rechtfertigen müssen. Das heißt an diesem Beispiel, nach einem Code of Conduct oder einer CDR, dass die Auswirkungen der Verwendung der Daten sich einer ethischen Grundprüfung unterziehen müssen, das muss in den großen Unternehmen verankert werden und das muss auch innerhalb dieser Unternehmen sanktionierbar werden. Stellen sie sich vor, wie Zuckerberg reagiert hätte, wenn der Aufsichtsrat gesagt hätte, ok wir möchten von Vorstand ein CDR-Konzept zur Einhaltung von Richtlinien, Code of Conduct, wie sich das Unternehmen verhält in solchen Fällen, und der Aufsichtsrat hätte Zuckerberg nach dem Fall um Cambridge Analytica einfach zwingend sanktionieren müssen. Da wäre der Druck intern für Zuckerberg viel größer gewesen, als einfach der Außendruck. Denn der Marktdruck ist da, dass wird Zuckerberg nicht aus den Fugen bringen. Aber wenn man internen

Druck und Sanktionen und man so welche Richtlinien in das GmbH oder Aktien Gesetz mit reinnehme, hat das einen ganz anderen Impact.

Florian Kugler: Das ist ein sehr interessanter Appell. Zeitlich müssen wir jetzt zur Nutzerperspektive rübergehen. Glauben Sie, dass die DSGVO dazu führt, dass wenn viele Opt-In-Verfahren eingesetzt werden, dass viele Nutzer den Opt-In verweigern werden?

Björn Stecher: Ne es wird eine Steigerung geben, durch die steigende Sensibilisierung, auch durch die DSGVO, Leute werden stärker darauf achten. Aber solange die Nutzer nicht genau wissen, was für einen Nutzen sie mit der Nutzung eines Produktes haben, werden sie weiterhin zustimmen, den Opt-In erteilen und nicht verweigern, ich glaube also nicht, dass in Zukunft wesentlich mehr Nutzer den Opt-In verweigern.

Florian Kugler: Ein weiterer wichtiger Teil der DSGVO sind die Betroffenenrechte, die gestärkt werden, wie Datenportabilität, ein sehr schwieriger Bereich in der Umsetzung. Auch Recht auf Löschung und Auskunft sind ja Bereich, die ein gewisses Verständnis erfordern. Werden Nutzer überhaupt diese Recht ausüben? Ist das sinnvoll?

Björn Stecher: Zwei Sachen. Wenn sie sich diese Gesetzt angucken, von der DSGVO sind sie fast deckungsgleich mit dem BDSG. Wir haben letztes Jahr oder vor zwei Jahren, haben wir gefragt ob Leute mal angefragt haben bei Unternehmen, wie diese mit ihren Daten umgehen. Die Zahl war verschwindend gering. Wenn ich unterwegs bin in dem Bereich, ich halte viele Vorträge, wenn ich nachfrage im Auditorium, wer kennt seine Betroffenenrechte, dann gehen von 100, drei Hände hoch. Das heißt die wenigsten wissen überhaupt, dass sie Betroffenenrecht haben und dass sie diese ausnutzen können. Da muss man auch erstmal wissen, ob man wirklich Betroffener ist. Zweitens was hat das für eine Konsequenz, wenn jemand mit den Daten irgendwie umgeht, das verlangt auch eine gewisse Kompetenz und die dritte Frage ist wie kann ich wirklich einfach meine Rechte ausüben, wer hilft mir da, muss ich da eine Email schreiben, muss ich mich da durch die Bestimmungen durchlesen, da gibt es viele Hürden. Der Marketeer weiß sich da wohl noch selber zu helfen, zu versuchen so wenig Barrieren wie möglich zu bauen, wie sind diese Barrieren zu schaffen. Deswegen glaube ich nicht, dass die Nutzer jetzt anfangen ihre Betroffenenrechte auszuüben, wir werden einen kleinen Peak haben dieses Jahr, wo viele damit aktiv konfrontiert werden mit dem Thema DSGVO. Dann wird es aber wieder abflachen und die Nutzer werden es nicht stärker ausüben so wie es gedacht ist. Und dritter Punkt, viele viele Nutzer wissen auch gar nicht welche Daten wie und wo gesammelt werden, Stichwort SmartTV, Internet der Dinge, mein eigenes Auto, viele beschäftigen sich gar nicht bewusst damit wo Daten gesammelt werden, wenn ich nicht weiß wo Daten gesammelt werden, weiß ich auch gar nicht ob ich der Betroffene bin oder nicht. Wenn ich das noch nicht mal weiß, dann werde ich keine Anfragen ausführen und Rechte geltend machen. Wenn was passiert, Leib und Leben in Gefahr ist oder die finanzielle Vermögenssituation in Gefahr ist, dann werden Leute

natürlich fragen, den Verbraucherschutz, aber ich glaube nicht, signifikant nach oben geht.

Florian Kugler: Eine Frage nebenbei. Was kann man den tun, um mehr Kompetenz zu schaffen, damit Nutzer den Markt besser zu verstehen?

Björn Stecher: Es ist ein Dreiklang, aufbauend auf den Gesetzten. Als Fundament die DSGVO, eine Säule ist der technische Datenschutz, der mit Datensicherheit zu tun hat, was auch damit zu tun hat, dass ich die Technologien nutze, die mir zur Verfügung stehen, um Datenschutz usable zu machen. Wie kann ich Tracking-Systeme nutzen um selber zu reflektieren wie mein eigenes Datenschutzverhalten im Internet ist. Zweitens der Vertrauensanker, die Materie wird so komplex sein, wird immer eine normative Unschärfe haben, dass sie nie abschließend für alle Stakeholder, ob Unternehmer, User oder Staat abschließend geklärt sein wird. Das bringt die Digitalisierung mit sich, verbindet die Lebensbereiche und es lässt sich die Komplexität nicht mehr in einem Gesetz abbilden. Sie werden also mit einer normativen Unschärfe konfrontiert. Wenn sie diese haben, müssen sie schauen wie sie Vertrauensanker schaffen. Vetrauensanker sind, dass die Gesetze entweder entflechtet werden, also zielgruppenspezifischer gemacht werden, also z.B. eins für den Datenhandel, eins für den öffentlichen Datenhandel, durch den Staat und Bürger, oder sie schaffen diese Schutzniveau-Kaskaden oder sie schaffen eine CDR, dass sie die Unternehmen dazu verpflichten CDR in ihren Unternehmen einzuführen. Und sie führen ein, dass es ein Datenethik-Framework gibt, dass eine gesellschaftlich austarierte und verhandelte gesellschaftliche Leitplanken gibt, die die Unternehmen einordnen. Dritt letztens gibt es die Kompetenz, die sie in den Schulen und Unternehmen ausrollen müssen. Das heißt aber auch Kompetenz ausbauen, Datensouveränität ausbauen, das heißt aber nicht, dass ich jetzt mit der Angstkeule komme, zu sagen wie schlecht Facebook und Google sind, und wir müssen uns da schützen, das ist nicht was ich meine mit Datensouveränität. Ich kann datensouverän sein und dabei diese Systeme nutzen. Weggehen von Grundsätzen wie Datensparsamkeit, so wichtig das ist, so verwirrend ist das auch für welche die sich nicht auskennen mit der Materie. Man sagt ja die Datenvolumina werden exorbitant steigen, auf der anderen Seite soll man sich datensparsam bewegen, das macht keinen Sinn. Sie haben so viele Denkblockaden drin, es wird nicht vom Nutzer aus betrachtet, deswegen muss Datensouveränität darauf abzielen auf die Frage, was habe ich für einen Nutzen wenn ich diesen Dienst wähle? Das ist eine ganz einfache, banale Frage, aber sie hat so viel Gewicht. Sobald ich weiß, was ich auf der Nutzenskala habe, dann kann ich such entscheiden, was ich aus meinem Datenportmonnaie auf die andere Seite lege, um dann wirklich auszutarieren, was hat das für mich für Risiko, was nehme ich und dann kann ich das viel besser und viel souveräner entscheiden. Und technisch, letzter Aspekt, es ist notwendig das wir

so ein personal Identifier Data Management System bekommen. Wie alt sind sie wenn ich fragen darf?

Florian Kugler: 25

Björn Stecher: 25, sie haben jetzt bestimmt mit 18 schon im Internet gesurft.

Florian Kugler: Ja.

Björn Stecher: Wissen sie da noch wo sie sich registriert haben?

Florian Kugler: Wahrscheinlicht nicht.

Björn Stecher: Ist auch nachvollziehbar. Wenn sie sich einen Halbkreis vorstellen bei dem Sie in der Mitte sind, dann geben sie immer Daten an Dritte aus, sie geben das raus, sie bekommen aber kein Feedback, und das wird sich in ihrem digitalen Leben immer mehr häufen, sie werden also gar nicht mehr wissen welche Daten sie vor 10 Jahren rausgegeben haben. War man spontan irgendwo eingeloggt, keine Ahnung. Das System muss man auf den Kopf stellen. Indem ich einen Datencontainer habe, Schnittstellen zur Verfügung stelle, wo Unternehmen auf diesen Container zugreifen, wenn sie Daten von mir haben wollen. Wenn sie das schaffen, kann ich als Nutzer mit Hilfe von Technologie einfach herausfinden, wer greift auf meine Daten zu, das wird protokolliert, ich kann das freigeben, ich kann auf der Siemens wo ich vor 10 Jahren gewesen bin, das läuft automatisch ab, bitte prüfen sie noch einmal ob sie den Datenbestimmungen zustimmen wollen oder nicht, es ist technisch heute alles keine Rocket Science mehr. Wenn sie das Prinzip umdrehen, dann können sie den Datenfluss behalten, es geht ja auch darum die Daten zu nutzen, das ist wichtig, aber sie haben viel Mehr Management Möglichkeiten, selbstbestimmt, proaktiv ihre Daten zu verwalten. Wenn sie das Menschen zur Verfügung stellen, dann wird auch automatisch die Kompetenz erwachsen, sich mit dem eigenen Verhalten auseinanderzusetzen. Das out oft he box, wenn sie fragen, wie man es besser machen kann.

Florian Kugler: Vielen Dank, das ist ein sehr interessanter Ansatz, auch sehr nutzbar im Verlauf meiner Arbeit. Vielen Dank für das Interview.

X.IV Experteninterview 4

Mo. 09.07.2018, 15:00 Uhr, Hamburg
Andreas Sierts
Senior Director AI & Analytics
Adform Germany GmbH

Begrüßung des Interviewpartners, kurze Vorstellung der Master Thesis und Einholung einer Einwilligung zur Aufzeichnung und Veröffentlichung des Leitfadeninterviews.

Florian Kugler: Hallo Andreas, vielleicht stellst du dich zunächst einmal vor und kannst im datenbezogenen Kontext schildern, wie Datenschutz dich und Adform als Unternehmen betrifft.

Andreas Sierts: Ich bin Andreas Sierts, ich bin Senior Director AI and Analytics. Ich kümmere mich zum einen um alles was mit Business Intelligence zu tun hat, also Datenanalysen intern und extern, als auch um Research, das heißt wo wir Daten unserer User dazu nutzen, Algorithmen zu verbessern, Optimierungen automatisiert durchzuführen, Machine Learning ist das Stichwort. Für uns als Adform ist das Thema Datenschutz natürlich total interessant, weil wir jetzt nicht erst seit DSGVO, sondern schon immer mit personenbezogenen Daten gearbeitet haben, wenn man jetzt voraussetzen würde, dass ein Cookie ein personenbezogenes Datum ist, spätestens seit der DSGVO ist es das. Ja wir arbeiten also mit personenbezogenen Daten, auch wenn es keine direkt personenbezogenen Daten sind, aber eben indirekt, deswegen ist Datenschutz da sehr wichtig. Wir arbeiten mit Kundendaten, wir arbeiten mit Order-IDs, also Bestellnummern, die dann zurückzuführen wären auf eine natürliche Person, wir haben IP-Adressen, auch wenn diese inzwischen abgeschnitten sind, aber das ist Grund genug sehr große Rücksicht auf das Thema Datenschutz zu nehmen aber besonders nachdem die DSGVO in Kraft getreten ist, mehr drauf zu gehen. Das heißt wir als Adform waren schon immer in der begünstigteren Position mit Unternehmen wie der Deutschen Telekom zu arbeiten, die per se schon sehr hohe Datenschutzanforderungen hatten, dass wir ein europäisches Unternehmen sind mit Sitz in Kopenhagen, unserer Server stehen in der EU, von daher waren wir bei dem Thema Datenschutz schon immer auf die EU gemünzt die schärfere Datenschutzrichtlinien hat als Amerika zum Beispiel. Und von daher waren wir relativ gut vorbereitet, ich sag mal 80/90% waren wir safe, aber trotzdem haben uns die letzten 10% noch einmal 1,5 Jahre und viel viel Arbeit gekostet, um bereit zu sein für die DSGVO, größtenteils sind das natürlich Dokumentationsthemen aber auch technische Systeme, die wir gewährleisten mussten, damit alles funktioniert. In dem Kontext wir stellen Technologie bereit, die es den Advertisern ermöglicht Werbung auszuspielen, in

diesem Zuge erfassen wir Daten, Cookie Daten, Behavioural Daten und so weiter. Und deshalb müssen wir da Rücksicht drauf nehmen.

Florian Kugler: Super, dann würde ich jetzt zum ersten Teil des Interviews kommen, nämlich der Relevanz der DSGVO. Es gab ja vorher auch schon die BDSG, es gab die Cookie-Richtlinie der EU. Hältst du eine neue Gesetzgebung hinsichtlich Datenschutz für notwendig? Also eine Überarbeitung durch die DSGVO.

Andreas Sierts: Ja, definitiv. Und wir haben auch von Tag eins gesagt, wir stehen hinter der DSGVO, weil wir es für super relevant halten und wichtig finden. Allein schon aus dem Grund, dass es bisher etwas gab, was aber sehr veraltet war, und es gab die ePrivacy-Richtlinie, die ja auch noch gilt, die aber teilweise sehr undeutlich ist indem was sie fordert, deswegen gibt es auch so unterschiedliche Auslegungen in den unterschiedlichen EU-Ländern, das ist immer noch so. Trotzdem wird das jetzt etwas nachjustiert durch die DSGVO. Weil es jetzt eben eine Verordnung ist, die für alle gleichermaßen gilt. Das gibt schon einmal Sicherheit, auch wenn das was zu tun ist, sehr umfangreich ist. Immerhin gibt es eine Sicherheit, die für jedes Unternehmen im Endeffekt gut ist, aber eben auch für den User. Da kommt der Punkt ins Spiel, dass wir als Technologie-Unternehmen was Werbung ausspielt, natürlich eine gewissen Vertrauensvorschuss der User brauchen. Das heißt, wenn am Ende des Tages alle Nutzer sagen, wir vertrauen den Unternehmen nicht mehr, die meine Cookie-Daten in irgendeiner Form erfassen oder verarbeiten, dann ist das ganze Geschäftsmodell des Online-Marketings irgendwann in Frage gestellt. Das heißt für uns ist es wichtig, dass die Nutzer verstehen was passiert, dass die Nutzer Transparenz haben, dass sie selber entscheiden können, welche Daten gespeichert werden und welche nicht und deshalb ist es total relevant und wichtig, dass da etwas passiert. Ob jetzt im Einzelnen jeder Abschnitt und jeder Satz perfekt ist, das sei dahin gestellt aber es ist wichtig, das das jetzt angegangen wird.

Florian Kugler: Zentral wird den Begriff der personenbezogenen Daten noch einmal verändert, es muss sich wahrscheinlich für den einzelnen Geschäftsbereich auch ableiten lassen, wie die DSGVO dann auch auszulegen ist. Hast du da konkrete Auswirkungen, die du da auf Online Marketing siehst, also auch ein bisschen in Hinblick auf programmatischen Einkauf und Retargeting?

Andreas Sierts: Also ganz konkret ist, dass Cookies, die Cookie-ID oder weitergreifend der Online-Identifier ein personenbezogenes Datum ist und wir das auch entsprechend zu behandeln haben, wie einen Namen oder eine Email-Adresse. Das hat per se erstmal keine Auswirkungen auf die Mechanik oder die Technologie, aber das hat schon Auswirkungen darauf, wie weit wir diese Daten einfach so nutzen können ohne den Nutzer zu informieren. Und deshalb haben wir als Adform gesagt, wir stehen hinter dem Standpunkt, wir brauchen auf jeden Fall eine Zustimmung des Nutzers dazu, dass wir einen Cookie setzen dürfen. Wie jetzt die Zustimmung aussieht, ist wieder unterschiedlich

geregelt in verschiedenen Ländern und das interpretiert auch jeder Webseiten-Betreiber und jeder Publisher wieder anders, aber es ist extrem wichtig, dass ein User seine Zustimmung gibt, dass wir Cookies setzen oder lesen dürfen. Das ist das eine. Und dann ist das Vertragsverhältnis zwischen uns, dem Werbetreibenden und dem Publisher, also den Webseiten, extrem wichtig, dass es klar ist, wo uns die Daten gehören oder wo wir die Daten nur prozessieren, das muss klar gewählt werden vertraglich, und das war eine der Hauptaufgaben, mehrere Tausend Partner Vertragsergänzungen zu schicken, in den klar geregelt ist, dass ihr (Partner ada.) von den Usern einen Consent einsammelt, also wir die Daten erfassen dürfen und einen Cookie setzen dürfen. Das war extrem wichtig für uns. Zum einen der vertragliche Gesichtspunkt, zum anderen der Technische, nur Daten dann verarbeiten, wenn der User auch seine Zustimmung gegeben hat.

Florian Kugler: Ja für euch als DSP oder Adserver, die meisten User wissen ja gar nicht, dass ihr existiert, dass da noch jemand zwischengeschaltet ist, der Cookies setzt, wenn jetzt ein Consent da eingeholt wird, die Cookie Banner sehen ja heute noch recht dünn aus, da stehen ja wenige Informationen zum Cookie, ich habe Studien gelesen wo steht, dass immerhin 50% der Bevölkerung im weitesten Sinne wissen was ein Cookie ist, das ist natürlich noch nicht genug. Wie sollte sowas dann aussehen? Wird sowas schon so umgesetzt, dass es DSGVO konform ist, oder sind wir da noch in einer Zwischenphase?

Andreas Sierts: Wir sagen ja, aber natürlich nicht für jede Website. Es gib unterschiedliche Auslegungen was zu tun ist, es gibt Webseiten, die sagen, wieso ePrivacy gilt doch noch, und in Deutschland informiert per Consent reicht, das heißt ich habe auf meiner Datenschutzseite stehen welche Anbieter ich nutze und da kann der User sich „ausopten“. Das ist ok, und dass muss man so akzeptieren, Es gibt andere, die sagen Cookie Notice ist ausreichend, wo drinsteht, dass Cookies gesetzt werden und man kommt weiter auf die Datenschutzseite. Die wahrscheinlich beste Lösung ist die, die auch von der IAB gefördert wird, dass das Cookie Window deutlich prominenter ist, bei dem Standpunkt stehen wir auch, zu sagen, es muss von dem Nutzer gesehen werden und nicht nur versteckt unten in der Ecke sein, es muss gut sichtbar sein und eine klare Information geben, dass Cookies gesetzt werden und wie diese verwendet werden. Und deshalb sind wir auch Bestandteil der IAB Consent Frameworks und bieten auch entsprechende Tools an, mit denen man Cookie-Hinweise auf Webseiten einbauen kann. Dass als Layer vor der Website oder ziemlich prominent unten steht, was passiert und wo man ins Detail gehen kann und lesen kann, welche einzelnen Zwecke einer Datenverarbeitung es gibt. Die Herausforderung besteht darin, dass das alles ziemlich komplex ist, also selbst wenn man es mit einfachen Worten beschreibt, ist es komplex und da kann man nicht gewährleisten, dass jeder User das versteht. Mir fällt auch nicht ein, dass man es so einfach erklären könnte, dass meine Oma es versteht. Das ist schwierig. Ich

glaube, dass es bis zu einem gewissen Grad zu einfacher werden kann, prominenter gemacht werden kann, aber irgendwann ist es dann so komplex wie es ist. Es sind viele Dienstleister, die involviert sind, die auch alle sinnvoll sind teilweise, für den Zweck warum ein Publisher oder Werbetreibender diesen Dienstleister verwendet, das ist dann eben so. Von daher, wir sind dafür das transparent und prominent zu kommunizieren.

Florian Kugler: Ja ich denke auch die Bewegungen eines Nutzers im Netz sind relativ flüssig und es gibt auch andere Lebensbereiche, wo man nicht alle Auswirkungen seiner Handlungen evaluiert, bevor man sie durchführt. Greift die DSGVO in deinen Augen zu kurz oder zu weit?

Andreas Sierts: Meiner Meinung nach ist die DSGVO in dem Scope in dem sie jetzt ist gut. Die Frage ist, wie die ePrivacy dann greift und wie da die Auswirkungen sind. Ich finde die DSGVO macht so schon Sinn und das sieht man ja auch daran, dass die USA sagt keine schlechte Idee, vielleicht machen wir auch sowas. Ob es jetzt kommt, weiß man nicht. Per se finde ich das schon in Ordnung so.

Florian Kugler: Welche Auswirkungen sind dann durch die ePrivacy Verordnung zu erwarten? Kannst du da schon sagen wann die kommt? Es geistert ja sowohl Ende 2018 als auch 2019 irgendwann im Raum rum?

Andreas Sierts: Das ist meiner Meinung nach noch sehr offen. Da müssen ja noch einige Runden gedreht werden. Ich denke auch eher, dass es 2019 wird, lassen wir uns überraschen. Ich glaube, dass die Auswirkungen vielleicht auf den Bereich digitales Marketing noch einmal größer werden, zum einen, wie ein Consent eingeholt wird in den unterschiedlichen Ländern und wie strickt und streng die einzelnen Länder sind. Da ist die Frage wird das nochmal klarer geregelt, dass alle EU-Länder, alle aus dem europäischen Wirtschaftsraum eben noch einmal einheitlicher das umsetzten, und dann ist die Frage was heißt einheitlich? Und da könnte es dann so sein das ein striktes Opt-In zukünftig da sein muss, und dann ist die Frage wie das eingeholt werden muss, und dann müssen wir uns überlegen, wie wir das umsetzen. Ich glaube das könnte interessant werden, wenn der Browser die Hoheit über das Opt-In hat, also wenn zum Beispiel der Chrome Browser von Google die Schnittstelle ist zu bestimmen, welche Dienstleister jetzt Cookies setzen dürfen und welche nicht, das halte ich dann für ein bisschen fragwürdig und das würde meiner Meinung nach zu weit gehen. Das kann man jetzt aber noch nicht absehen. Was gut ist, das Consent-Framework, die Technologie, das ist bereits so gebaut, dass es eine etwaige Opt-In-Regelung möglich wäre darüber umzusetzen.

Florian Kugler: Stichwort Browser Technologie. Wenn man an Chrome denkt, einen seh verbreiteten Browser, der ein Teil von Google ist, die DSGVO wirkt sich natürlich auch immer etwas auf den Markt aus. Und Google hat ja einen riesen Marktanteil, von

Teilweise 90%. Google und Facebook dominieren ja schon sehr stark den Online-Werbemarkt. Siehst du da Auswirkungen auf das Gefälle, auf das Machtgefüge?

Andreas Sierts: Naja zum positiven und zum negativen für diese Anbieter. Also zum Positiven ist, dadurch, dass sie so eine Macht haben, können sie sich auch viel rausnehmen, das heißt wenn Google sagt wir machen die Schotten dicht, wir erlauben nicht mehr, dass andere auf YouTube mitmessen wegen GDPR (DSGVO), dann wird das größtenteils so akzeptiert, ich sehe nicht, dass da jetzt größere Budgets abgezogen werden, ist aber natürlich nicht was ich als Werbetreibender will, nämlich, dass eine unabhängige Prüfung möglich ist, was dann nicht mehr der Fall ist, das ist eigentlich nicht korrekt, für Google jedoch sehr gut, da keiner mehr ihre Arbeit überprüfen kann. Das könnte die negative Auswirkung der DSGVO sein, dass einige Anbieter das ausnutzen, um die Schotten weiter hochzuziehen. Und dann wäre es schlecht. Positiv, man sieht schon, dass die Anbieter unter Druck geraten, ob es durch Cambridge Analytica ist, ob es die DSGVO ist. Wir sehen jetzt auch, dass Google nicht alles machen kann, es kam vor Wochen ja die Idee von Google auf, wir machen ein Consent-Tool, wir holen uns selber den Opt-In der User ein, dass können die Publisher aktivieren, und übrigens es sind nur 10 verschiedene Dienstleister auf dieser Liste erlaubt, weil Forschungen gezeigt haben, mehr wollen die User eh nicht, verstehen die User nicht, was das für Anbieter sind, deswegen nur 10 auf der Liste. Es gibt natürlich viel mehr als 10 Anbieter im AdTech Bereich, das heißt das würde befördern, dass Google die eh auf dieser Liste sind, und die anderen größten Dienstleister in den jeweiligen Ländern und nicht die kleinen Anbieter, das wäre der Todessturz für alle kleinen Unternehmen, alle Start-Ups im Bereich AdTech, wenn Google dafür der Filter wäre, für wen jetzt ein Consent eingeholt werden kann und für wen nicht. Da gab es dann so viel Druck aus der Industrie, dass Google das dann zurückgenommen hat und daran sieht man auch, was passiert wenn die Industrie zusammenhält gegen Google. Ein anderes Beispiel ist das Consent-Framework von der IAB, erste wollte Google mitmachen, dann wieder nicht und jetzt sieht es so aus als würden sie wirklich teilnehmen, da sieht man auch den Druck der von außen auf Google lastet, so unerheblich ist der nicht, so dass sie dann auch mal zurückrudern. Es geht nicht, dass ein Anbieter macht was er will, ohne Kontrolle von außen, durch den Deckmantel von GDPR entsprechende Entscheidungen getroffen werden, die nur diesem Anbieter nutzen.

Florian Kugler: Von Google und Facebook lässt sich sehr gut die Brücke zum Nutzer schlagen, da es ja sehr große Ökosysteme sind in denen sich Nutzer seinen Consent vielleicht schon mit dem Login gibt und dann bleibt er drin. Und daran sind ja viele mitlesende Algorithmen gekoppelt und zum Beispiel die Ausspielung von personalisierten Werbebannern. Generell, glaubst du, dass Nutzer in Zukunft den Opt-In in großem Maße verweigern werden?

Andreas Sierts: Ich glaube es wird schon mehr geben, die es verweigern werden. Es komm immer drauf an, welche Auswirkungen das dann auf den User hat. Wenn er merkt, huch, das Internet funktioniert jetzt nicht mehr wie ich es kenne, wenn ich verweigere, dass Cookies gesetzt werden dürfen. Ich kann mir schon vorstellen, dass viele weiterhin ihren Opt-In geben werden. Wie wir halt gesehen haben, dass ein User wenn er einen Opt-IN gibt auch für alles einen Opt-In gibt und nicht in die Liste geht und sagt hierfür gebe ich einen und hierfür nicht. Es wird aber schon einen signifikanten Anteil geben, der kein Opt-In gibt.

Florian Kugler: Facebook hat ja massig Nutzerdaten, die sie erheben im Netzwerk und darauf basierend Target Groups ihren Werbekunden zur Verfügung stellen, die dann auch mit Third Party Daten der Werbekunden gekoppelt sind, statistische Zwillinge etc., da geht man ja was die Datenvielfalt angeht über das Netzwerk hinaus, für eCommerce Unternehmen zum Beispiel. Sind da Veränderungen zu erwarten oder wie ist das zu behandeln? Auch in Sachen Kopplungsverbot.

Andreas Sierts: Also zum einen ist zu hoffen, dass die Unternehmen in Zukunft strenger mit ihren Daten umgehen werden, dass sie nicht blind alles zu Facebook hochladen. Und dann ist die Frage wie man es macht, ich kann ja unabhängige Drittanbieter dazwischenschalten, die zumindest die Daten so pseudonymisieren, dass Facebook nicht nachvollziehen kann wer dahintersteckt, welche Informationen dahinterstecken. Ich muss also Unternehmen viel genauer darauf schauen, was ich mit welchem Anbieter mache und wie ich es mache. Da glaube ich fest dran, nicht erst seit Cambridge Analytica, auch vorher war das schon ein Thema. Ich glaube das Reputationsrisiko für solche Unternehmen ist viel zu hoch, als dass sie irgendwas wagen werden, was am Ende schief gehen könnte. Ich glaube am Ende des Tages wird es gerade bei einem Facebook, dass viele Profilbezogene Information hat über seine Nutzer, da wird es extrem relevant, auch bei Google, bei uns ist es nicht ganz so relevant, weil wir eben keine eigenen Daten haben, keine personenbezogenen Nutzerdaten. Wir sehen von den Kunden der Unternehmen nur IDs, wir wissen ja Garnichts von den Nutzern, vielleicht die Surf-Historie sag ich mal, aber nicht was mit direkt personenbezogenen Daten zu tun hat. Von daher denke ich schon, dass die Unternehmen da noch sensibler sein werden, was jetzt die eigenen Daten angeht, und das ist auch gut so.

Florian Kugler: Ihr speichert ja Cookie-Daten, IP-Adressen etc.. Jetzt gibt es zur BDSG in der DSGVO noch einmal deutlich gestärkte Betroffenenrechte, und relativ neu ist die Datenportabilität, das Recht auf Löschung wurde ja nochmals präzisiert und gestärkt. Werden Nutzer ihre Betroffenenrechte nun auch ausüben?

Andreas Sierts: Ist es zu erwarten? Ja. Werden es viele machen? Nein. Das ist auch was wir in den ersten Wochen sehen, in den ersten 5 Tagen nach dem In Kraft treten hatten wir 2,3-X Anfragen zu dem Thema, aber dann ist das auch wieder abgeebbt. Wir

immer bei so einem Thema, wenn es gehyped wird, dann gibt es welche die das testen wollen, das sind dann welche, die damit etwas zu tun haben, sich sehr darum kümmern um ihren Datenschutz. Ansonsten ist nicht zu erwarten, dass eine große Flut kommt. Was wichtig ist, wir müssen alle Grundlagen dafür schaffen, dass diese Rechte auch benutzt werden können. Also wenn der Nutzer das Recht ausübt, dass seine Daten gelöscht werden, dann machen wir das auch. Viele Nutzer verstehen dabei nicht, dass wenn sie eine E-Mail-Adresse mit ihrem Namen schicken, dass wir ihnen Garnichts zuschicken könne, weil wir den User nicht kennen unter seinem Namen und seiner Email-Adresse. Sofern der User nicht seine Cookie ID mitschickt, können wir nichts damit anfangen. Das heißt bei uns gibt es die Methodiken all das zu tun, wichtig ist aber auch wie der Nutzer da macht. Deswegen haben wir ein eigenes Privacy-Center auf unserer Homepage, wo der User von seinem Browser aus das beantragen kann. Da lesen wir die ID aus dem Browser aus, geben sie ans System und löschen die Daten. Das muss gewährleistet sein. Ichglaube aber nicht, dass das wahnsinnig viele Menschen machen wollen.

Florian Kugler: Sehr lobenswert jedoch, dass ihr das bereit stellt und der Nutzer das selbstbestimmt seinen Opt-Out vornehmen kann.

Andreas Sierts: Ja genau, seit Tag 1 ist das möglich bei uns, und das funktioniert auch, wenn ein User das möchte, machen wir das auch.

Florian Kugler: Um zur User-Experience zu kommen, zum Thema Cookie Banner und erweiterter Consent, wenn Seiten nicht vollständig geladen werden können, weil auch da schon Cookies gesetzt werden, was ist da zu erwarten, vielleicht dann auch umgesetzt durch die EPrivacy-Verordnung. Wird die User Experience dann sehr stark darunter leiden?

Andreas Sierts: Ja, was zu erwarten ist können wir auch noch nicht sagen. Es gibt unterschiedliche Entwicklungen. Die Entwicklung, wenn der User nicht zustimmt bei der Abfrage, kommt er gar nicht vorher auf die Website, das ist natürlich sehr streng. Oder wenn der User nicht zustimmt, gibt es keine Werbung. Da stellt sich die Frage, ob die Webseiten das durchhalten, die auch auf Werbung angewiesen sind. Das ist eine Tendenz die wir sehen. Eine andere Version sieht so aus, dass die Information so übermittelt wird, dass sie den Ablauf nicht direkt stört. Es gibt bereits einige EU-Länder, die sagen, dass das Weitersurfen Consent genug ist, auch weiterhin. Da sind wir gespannt wie das von der EPVO interpretiert wird und aufgenommen wird und ggf. Dann nicht mehr möglich ist. Ist natürlich für die UX ganz schön, denn der User muss nicht aktiv klicken und wird nicht gestört. Am Ende gibt es da unterschiedliche Entwicklungen und ich kann nicht voraussagen was da passieren wird. Persönlich finde ich schon, dass am Ende die Information irgendwo transparent sichtbar sein muss, aber ich glaube nicht daran, dass

man vor jedem Webseitenbesuch eine Horde an Opt-Ins anklicken muss, um die Webseite zu sehen. Das ist auch nicht im Sinne des Nutzers.

Florian Kugler: Ihr bezeichnet auf eurer Webseite Audience und Behavioural Data als die Währung der Zukunft. Was auch eine interessante Frage ist, wie kann dieser Wert auch auf Nutzer zurückgeführt werden? Es hat natürlich einen Mehrwert, personalisierte Werbung nehmen manche Nutzer auch als Mehrwert auf, andere wieder nicht. Man kann ja theoretisch einen Opt-Out in Zukunft wählen und kriegt nur noch Werbung mit der Gießkanne oder im Umfeld platziert. Gibt es da einen Weg diesen Wert auch auf Nutzer zurückzuführen, einen besonderen Mehrwert zu generieren.

Andreas Sierts: Da gibt es unterschiedliche Ansätze. Es gibt ja schon Unternehmen, die sich darauf spezialisiert haben, an den Nutzer Geld weiterzuleiten. Wenn ich meine Daten Verkaufe, bekommen ich auch was, entweder einen Euro-Betrag oder Punkte. Da glaube ich nicht dran, aus dem einfachen Grund, weil die Anzahl an Werbeeinblendungen mit meinen Daten müsste so riesig sein, dass sich das lohnt. Das ist unrealistisch. Ich glaube nicht, dass der User am Ende incentiviert werden kann, über monetäre Aspekte oder sonstiges, um das zu machen. Der Aufwand das alles zu pflegen ist einfach zu groß, als dass der Nutzer einen Nutzen davon hat. Wenn man sich die TKP Preise anguckt, die sind so gering im Verhältnis, da kriegt der Nutzer 5,40 € überwiesen am Ende des Monats, das ist zwar nett aber auch nicht Anlass, groß etwas dafür zu machen. Du hast ja am Anfang schon das Paradoxon angesprochen, eigentlich ist mir das wichtig, aber ich will mich nicht drum kümmern, und das spielt da mit rein. Da ist eher so die Frage, auch bzgl des Kopplungsverbots, das mein Zugang zur Website nicht verweigert werden darf, das ist also auch schon mal raus, die Frage ist eher, wie wird sich das ganze Thema bezahlte Zusatzangebote entwickeln? Es könnte dahin gehen, dass wir eine Art Zweiklassengesellschaft haben. Einmal diese per Login bezahlten Angebote auf der anderen Seite die freien Angebote, wo eben nicht mit Usern und Cookies gearbeitet werden darf, da darf der User dann entscheiden reicht mir das aus, was ich in den freien Angeboten habe, oder habe ich das AdOn mehr Information für die ich dann auch bereit bin zu zahlen. Was hat der User dann am Ende davon? Ich weiß es nicht was dabei rauskommen wird. Ich glaube, dass die Nutzer den Mehrwert von Werbung zu schätzen wissen, wenn es eben keine Werbung mehr gibt. Und da kann man nur über Aufklärung machen, dass kann man nur drüber machen, dass die User ein Vertrauen in Unternehmen haben, die Daten erfassen und sammeln. Ansonsten fällt es mir schwer, rauszufinden, was der Incentive für den User sein könnte. Bei einem Netflix oder Amazon weißt der User was er davon hat, dass Daten erfasst werden, da gibt es bessere Angebote, bessere Empfehlungen. Das ist noch nicht so ganz klar für die meisten Nutzer, dass das im sonstigen Internet auch so ist. Ich glaube, wenn man das weiß ist das bereits ein

Incentive, da muss man dann aber eben noch mehr machen in der Transparenz und der Konfigurierbarkeit. Das muss alles einfach und unaufwendig sein.

Florian Kugler: Dann sind wir auch schon am Ende angekommen. Fällt dir als Schlusswort noch etwas ein was du ergänzen würdest?

Andreas Sierts: Das ist eine sehr gute und positive Entwicklung, die das eingenommen hat. Und ich glaube, dass wir als Unternehmen noch viel stärker auf das Thema eingehen müssen. Ich glaube aber, dass noch keiner den Weg gefunden hat der beide Seiten gleichermaßen befriedigt. Ich als Publisher oder Webseite muss irgendwie Geld verdienen, ich als User will so wenig preisgeben wie möglich, das muss man irgendwie in Einklang bringen. Das zweite ist, auch wenn viele Nutzer nicht zustimmen, glaube ich, dass Online Marketing trotzdem nicht sterben nicht, es gibt auch genug Wege OM nutzbar zu machen, auch ohne nutzerspezifische Daten, ob das jetzt kontextuelle Themen sind oder über Panels, da wird es viele Möglichkeiten geben, die besser sind als das, was wir vor 30 Jahren hatten ohne Cookies. Ich glaube wir gehen nicht zurück in die Zukunft.

Florian Kugler: Dann vielen Dank für das interessante Interview.

Andreas Sierts: Ja, gerne.

X.V Gruppendiskussion Nutzerverhalten und Datenschutz

Sa. 14.07.2018, 20:30 Uhr, Hamburg

6 Teilnehmer (anonym)

Begrüßung des Gruppendiskussionsteilnehmer, kurze Einweisung in den Gesprächsverlauf und die grundlegenden Diskussionregeln.

Moderator: Willkommen, wir starten jetzt mit der Gruppendiskussion. Die erste Frage lautet, welche digitalen Dienste nutzt ihr regelmäßig und warum?

T2: Dienste?

Moderator: Noch einmal um digitale Dienste einzuordnen. Das können Apps sein, Webseiten, Betriebssysteme, E-Mail-Accounts, Smart Home Technology, also was ihr regelmäßig oder wöchentlich benutzt. Also vielleicht die drei Sachen, die ihr am meisten benutzt.

T2: Soll ich anfangen? Also ich glaube ich spreche für alle, wenn ich sage Whatsapp, mit Abstand am meisten, als zweites würde ich Reddit sagen, als die Plattform, wo ich nach Whatsapp am meisten drauf bin und Social Media mäßig halte ich mich eher zurück. Darum kommt danach wohl schon mein E-Mail-Provider.

Moderator: Welchen E-Mail-Provider?

T2: Yahoo , ganz Old School.

T4: Also wenn ich in mein Handy gucke und die Verbrauchsdaten angucke, was ich am meisten benutze, dann ist es erschreckender Weise bei 40% Instagram…

T3: Bei mir auch.

T6: Bei mir auch.

T1: Da gehen Bilder natürlich auch stärker aufs Datenvolumen als anderes.

T4: Ich merke das aber auch bei mir, ich bleibe kleben. Mittlerweile gibt es die Möglichkeit, das ist dein Newsfeed, bis dahin hast du ihn schon geschaut und dann legst du es mal bei Seite. Aber Instagram ist schon die Haupt-App, irgendwelche Sport-Apps, vielleicht Runtastic, nutze ich ab und an, wenn ich laufen gehe. WhatsApp natürlich auch aber am meisten diese „Gesehen und Gesehen werden“ Geschichten auf Instagram.

T6: Vielleicht muss man es auch trennen zwischen privat und beruflich, beruflich bin ich auch viel in anderen digitalen Sphären unterwegs. Obwohl es ist auch viel Facebook.

T3: Ja Facebook.

T4: auch viel Facebook.

T3: Facebook weniger, aber als erstes Instagram, dann WhatsApp und Email an dritter Stelle. Das sind so die Apps die immer offen sind.

T5: Wir haben bei uns jetzt Asana eingeführt, dass ist so eine App für Projektmanagement, da sind wir auch viel unterwegs. Und letztendlich E-Mail-Dienst, WhatsApp und Asana jetzt beruflich.

T1: Wobei da gibt es jetzt tausend andere Apps, die man nicht nennt und die man im Verlauf des Tages irgendwann mal aufmacht und dann gibt es welche, die hast du die letzten Jahre nicht aufgemacht, die dann irgendwann mal runterfliegen.

T4: Auch Amazon nutzt man ja viel, eBay, eBay Kleinanzeigen.

T2: Da würde ich jetzt aber nicht sagen, dass ich das in einem geregelten Zeitabstand nutze. Nur vielleicht wenn man gerade einzieht.

T5: Google Maps vielleicht noch.

T3: ja Google Maps.

T2: Google Maps nutze ich täglich.

T6: HVV nutze ich auch viel, gar nicht wenn ich die Wege brauch, sondern um zu gucken wann die beste Verbindung ist.

T1: Das mache ich gar nicht mehr, das habe ich an Google outgesourced. Ich gehe nie wieder auf diese Seiten.

T3: Ja das macht ja Google, Google Maps sagt dir das. Das hast du auch in jeder Stadt, ob Düsseldorf oder München, ich bin ja auch beruflich viel unterwegs und guck mir die Strecke an und gehe auf Bahn und dann übersetzt er das ja in die HVV oder BVG App.

Moderator: Viele Services sind ja schon genannt. Nutzt ihr viele Google Produkte?

T6: Ja Mail.

T2: Ja ich nutz auch geschäftlich Google Mail. Privat auch nur noch Google Mail.

T2: Auch drive.

T3: Google Mail, Maps, Drive, Kalender…

T4: Hang Outs

T2: Ja Hang out werden viel genutzt

Moderator: Google und Facebook Produkte nutzt ihr anscheinend am meisten in den ganzen Bereichen, warum ihr nutzt ihr diese mehr als die Konkurrenz?

T6: Weil Google so omnipräsent ist. Ist für mich meine Suchmaschine Nummer 1, und dann bietet es sich an Google auch für Mail etc. zu nutzen. Und dann wiederum benutze ich Google bei der Arbeit, wir haben in der Uni Google Mail und da hat man dann nicht verschiedene Anbieter, sondern es ist zentriert auf einen.

T3: Plus, du bist mit deinen ganzen Kontakten verknüpft, ich habe zum Beispiel die Kalender von anderen bei mir im Kalender drin, unsere Kalender sind über Google Mail verknüpft und dann kann ich deren Termine einsehen.

T1: Ich würde sagen, ich wüsste gar nicht auf Anhieb wen ich jetzt noch als Konkurrenten von Google ansehen würde…

- Allgemeines zustimmendes Lachen –

T1: Yahoo hat ja mal versucht es zu sein viele Jahre und war früher glaube ich mal größer, ist aber inzwischen ja enorm zusammengeschrumpft, von daher hat es ja nicht mehr die Bandbreite an Produkten wie Google es hat.

T3: Ich wüsste gar nicht was eine Alternative wäre.

T1: Ich hab Mail, ich habe Drive, ich habe Kalender, das ist die Seite auf der ich eh sein will.

T6: Jetzt auch für meine Abschlussarbeit.

T4: genau Google Books für die Thesis, mir fehlt irgendeine Kleinigkeit, irgendein Zitat, dafür ist Google Books echt super.

T1: Da finde ich Facebook ist deutlich eher angefochten bei mir als Google…

T6: Vor allem mittlerweile

T1: Da gibt es andere Sachen, auf die man zurückgreifen kann. Man braucht den Messenger nicht, da hat man WhatsApp, den Kalender, wenn du wirklich mal nicht die Geburtstage deiner Freunde aufschreibst

T2: Whatsapp ist ja Facebook und da gibt es mehr die Konkurrenz zu Telegram und da ist eher mein Punkt die Datensischerheit, und da ist der letzte der Gehackt wird meiner Meinung nach Google, also vorher wird jeder andere Gehackt, als dass jemand meine Daten von Google klaut, denn da arbeiten die besten Informatiker und so weiter und sofort, die geben ja riesige Prämien raus, wenn da einer Sicherheitslücke gefunden wird. Also von der Datensicherheit ist Google de absolute Topspot und da würde ich bei Facebook eher sagen, WhatsApp würde ich viel weniger benutzen, wenn viel mehr Leute Telegram benutzen würden, einfach aus dem Grund, dass ich weiß, dass Facebook meine Daten verkauft, Google nutzt sie zwar auch, klar weil sie auch ein riesiges Marketing Büro sind, mit Google Ads, habe aber mehr im Gefühl, dass das inhouse bleibt, ich weiß auch nicht. Vom Gefühl, wenn Google meine Daten benutzt, für eigenes Marketing, wo andere Leute sich einkaufen bei denen, erfahren die das wenigstens nicht, aber Facebook verkauft das halt frei an Dritte weiter.

T6: Das liegt aber auch an den schlechten Medien über Facebook, da ist man jetzt verunsichert.

T3: Ich finde bei Facebook ist es mir schon egal, da habe ich das Vertrauen eh schon verloren, da sind keine Daten, die mir wichtig sind, ich benutze Facebook bei allen Apps die ich verwende, z.B. Runtastic. Mit Facebook anmelden? Ja passt.

T4: Facebook ist so die Ramsch E-Mail-Adresse von früher.

T3: Das ist die Ramsch-Email-Adresse, ich benutze es überall und da sage ich, dass haben die ehe schon, dass können sie haben.

T1: Facebook ist für mich keine Ramsch-E-Mail. Ich sage nie mit Facebook anmelden, weil dann haben sie direkt deinen vollen Namen, vielleicht noch deine Adresse, und

vielleicht hast du deine Handynummer hinterlegt, also mit Facebook anmelden ist das Gegenteil von einer Ramschmail.
T6: Das finde ich auch.
T1: Also Datenschutz mäßig.
T4: Du behandelst sie als wäre es deine Ramsch-E-Mail-Adresse, als würdest du deine erste Hotmail-Adresse von früher nehmen und da hast du im Posteingang 10.000 ungelesene Mails die da drin sind.
T1: Aber trotzdem schmeißt du ja gleichzeitig deine Daten mit.
T4: Adresse habe ich bei Facebook nicht hinterlegt. Und auch meine Handynummer nicht.
T3: Ich habe nicht einmal mein Geburtsdatum drin, nur den Tag, ohne Jahr glaube ich, irgendwie so.
T5: Bei Facebook ist man auch mit allen verbunden, Facebook sammelt da richtig viele Daten. Und da denke ich immer, wenn ich mich irgendwo anmelde, dann ist das noch so ein riesen Schwanz mit dran, als wenn ich mich mit einer E-Mail anmelde.
T1: Das denke ich auch. Dann kriegen deine Facebook Kontakte direkt die App angeboten, die du dir gerade runtergeladen hast.
T5: Welche Seiten du besuchst und wo du warst (physisch), das hängt da alles mit dran.
T3: Also ich glaube auch, dass das nicht klug ist, das denke ich auch. Aber das ist einfach so drin, das ist so einfach. Wenn du einfach mal ne App runterlädst.
T4: Facebook war irgendwie als erstes da und darauf kannst du immer wieder zurückgreifen. Ich glaube jeder hat ein Facebook Konto und da ist es die einfachste Lösung, vielleicht nicht die intelligenteste, aber die einfachste, und deswegen wählt der Großteil diesen Weg.
Moderator: Ihr habt die zweite Frage jetzt auch schon gut beantwortet, nämlich welche Privatsphärebedenken ihr bei der Nutzung dieser Dienste habt, da seid ihr nahtlos reingeschliddert, ohne dass ich das anleiten musste, habt ihr sonst noch weitere Privatsphärebedenken bei der Nutzung dieser Dienste, also ihr habt gerade schon gesagt bei Facebook man schon eher das Gefühl hat, dass Daten da auch für andere Zwecke benutzt werden, bei Google fühlt sich ein Teil der Gruppe sehr sicher, habt ihr
Generell Privatsphärebedenken bei eurer Internetnutzung?
T4: Überall, bei allem was ich mache.
T3: Ja.
T6: Und es wird auch immer stärker, und es gibt immer mehr Beispiele. Zum Beispiel bei der Benutzung meines Handys, beruflich und privat, da wird Beispielsweise die Werbung ausgespielt, die ich beruflich hoch lade bei Instagram, und ich bekomme sie in meinem privaten Konto, obwohl ich weiß, dass ich eigentlich nicht die Zielgruppe bin. Da gibt es viele Zufälle, die sehr strange sind. Auch wenn ich über Sachen rede, dann

kommt auf einmal die personalisierte Werbung, auch wenn man nichts in die Suchmaschine eingegeben hat.
T3: Ich finde es gruselig aber irgendwie akzeptiere ich das so.
T4: Ich akzeptiere das auch. Du musst ja irgendwie Digital Player sein, du kannst in der heutigen Welt vernetzt sein.
T3: Wenn du die Dienste nutzen willst, kommst du nicht drum herum, deine Daten da ein Stück weit zu lassen.
T4: Wenn es jetzt keine Nacktbilder von mi sind, ist mir das auch egal.
T6: Habt ihr eure Kameras abgeklebt?
T3: Ja. Laptop ja, Handy nicht.
T5: Habe ich mal gemacht, aber dann ist das abgefallen und dann war es mir auch egal.
T4: Dann brauchst du auch keine Selfies mehr machen, entweder du machst es komplett und machst es am Telefon auch oder du lässt es ganz.
T2: Dein Handy ist ja hauptsächlich in deiner Hosentatasche.
T4: Dein Handy ist hauptsächlich in deiner Hosentatasche? Das glaube ich nicht. Dein Handy ist hauptsächlich hier vor deinem Gesicht. Bei mir zumindest und bei vielen.
T5: Nochmal zurück zu diesem Price you have to pay, wenn man da mitmachen will. Also ich finde es schon gruselig, wenn da die ganze Zeit das Mikro mitläuft. Da habe ich letztens auch nur mal was vor mich hingesagt, weil es mich interessiert hat, ob mein Mikro mithört und dann habe ich es in Google eingegeben, und dann kam genau das. Naja und das heißt ja, dass selbst wenn ich es nicht benutze es 24/7 mithört und da Daten abgefangen werden, und ich finde das einfach echt nicht ok so.
T1: Ne.
T2: Ne das finde ich auch überhaupt nicht ok. Nur weil es einmal auf „Hi Siri“ oder „Ok Siri“ reagieren kann, das ist einfach eine schlechte Ausrede für Apple einfach bei allem mitzuhören.
T1: Ja das finde ich auch.
T4: Das Mithören ist auch echt was anderes, das finde ich auch nicht gut.
T2: Da kann man ja wirklich nichts gegen machen.
T5: Außer man hat ein spezielles Telefon.
T2: Aber wer hat schon ein Silent Phone, aber das ist halt spezialisiert darauf, das alles komplett abzuschirmen.
T3: Das sie aktiv, wenn du auf Sachen klickst, Dinge likest, dann finde ich es OK wenn sie dich verfolgen, aber wenn man mit Freunden irgendwo sitzt, da wäre für mich dann der Unterschied.
T4: Das ist ja auch so, dass wenn man Google Maps offen hat, und nicht wieder geschlossen, da bin ich am Barmbeker Bahnhof ausgestiegen und war bei Penny eikaufen gewesen, das mache ich normalerweise nie, ich gehe immer zu Edeka. Da war es so,

dass kurz danach, Penny Werbung, was ich nie vorher hatte, bei Instagram hatte. Das lag wohl daran, dass ich mit der offenen App da einkaufen war.
T3: Wenn die App zu ist können sie das dann nicht?
T4: Weiß ich nicht.
T3: Ich mache meine Apps immer zu.
T4: Du kannst auch die Ortungsdienste ausschalten, was au Android deutlich leichter geht, als auf bei Apple.
T3: Ich habe Ortungsdienste auch nur beim Verwenden der App aktiviert. Und wenn ich es dann schließe, dürfte es ja eigentlich nicht so sein.
Moderator: Ist euch Datenschutz wichtig?
T6: Ja.
T5: Ne.
T4: Ja eigentlich. Wir sagen wir machen es trotzdem alles, Das ist ein wenig schwierig, eigentlich ist es wichtig aber man nutzt trotzdem alles und verzichtet darauf sein Daten zu schützen.
T3: Das ist so widersprüchlich.
T4: Es ist allen so wichtig und jeder spricht darüber…
T3: … keiner tut was dagegen.
T4: Ich bin gerade wieder bei Facebook oder Instagram, es ist mir egal. Ich lasse die App offen, ich klebe meine Kamera nicht zu.
T1: Ich verlasse mich schon deutlich eher drauf zu kontrollieren, was ich einpflege, als das was irgendwohin geht. Ich glaube den Kanal haben wir eben ausführlich besprochen, der lässt sich nicht mal wirklich nachvollziehen, verstehen vielleicht, man weiß gar nicht an welchen Ecken abgegriffen und verwertet werden, aber ich würde schon sagen, dass wie T4 spaßhaft gesagt, solange keine Nacktbilder von mir im Internet sind, ist mir das eigentlich recht. Solange jemand nur weiß wie alt ich bin und dass ich aus Hamburg komme und dann wo ich studiert habe und wo ich arbeite, dann kann er von mir aus auch auf Bilder drei Freunde identifizieren, das finde ich eigentlich in Ordnung. Ich verstehe, dass so etwas gesammelt wird, weil es Industrien gibt, die mit den Daten was anfangen könne. Man hat dafür einen gewissen Komfort und ich würde versuchen eher die Seite zu kontrollieren, dass man versucht nur die Daten preiszugeben, bei denen man letztendlich auch OK findet oder verkraften kann, wenn sie öffentlich sind.
T3: Ja.
T6: Ja
T5: Also ich finde, wenn es auf der individuellen Ebene ist, dann OK keine Nacktbilder von mir, dann ist das ok so. Aber gerade was man jetzt bei der US-Wahl gesehen hat, was auch beim Brexit der Fall war, dieses Microtargeting. Da finde ich das eben sehr kritisch, wenn es de einzelne ist. Der hat nicht so einen großen Schaden davon, wenn

aber Marketing-Instrumente aufgefahren werden kombiniert mit psychologischen Modulen. Und man da wirklich politische Entscheidungen mit beeinflussen kann, dann ist es gruselig und einfach auch eine riesengroße Waffe.

T6: Ja das finde ich auch, eine riesengroße Waffe.

T4: Der Mensch ist auch nur soweit lenkbar, wie er es auch zulässt.

T6: Das ist ja der Punkt, den T5 angesprochen hat, es hat ja keiner zugelassen, sondern da hast du ja kaum noch eine Chance. Und wenn man ganze Wahlen damit beeinflussen kann, wer weiß was noch alles geht mit Daten.

T4: Wenn du eine gefestigte politische Meinung hast, dich einmal positioniert hast, dann wechselst du nicht auf einmal ins andere Lager.

T2: Doch die kann sich schon bilden über mehrere Jahre langes Bombardement auf Facebook.

T4: Ja wenn es ein Projekt über Jahre ist…

T2: es ist ja ein Projekt über Jahre, Regierungen denke lange. Also Putin hat ja auch nicht 2 Monate vor der Wahl damit angefangen die Nutzer mit Trump Werbung zuzupflastern. Ich glaube wenn das alles bestätigt wird.

T4: Rein hypothetisch.

T5: Was ich noch sagen wollte, wenn man das so zulässt. Ich meine Apple hat isch auch aufgebaut über Jahre, wenn man schon heute die Assoziation hat, dass man zu einem Tablet iPad sagt und zu einem Laptop, Macbook, dann hat sich das einfach festgesetzt im Kopf. Apple steht heut einfach für etwas hochwertiges, auch wenn es auf der technischen Seite viel dagegengesprochen wird. Das geschieht subtil über Jahre. Wenn man wirklich die Macht hat das alles abzuhören und zu verarbeiten, dann kann man damit auch riesengroßen Schaden oder auch Einfluss damit gewinnen.

T4: Generell Einfluss, das stimmt. Aber ich glaube es gibt die Leute die dafür anfälliger sind und andere weniger. Gerade in Amerika ist es, wo wir gerade über die Politik gesprochen haben und wo es ja auch um Datenschutz ging, da sind die Leute auch einfach beschränkter, da sind sie nicht weitsichtig genug. Die haben kein politisches Weltbild, sondern sehen nur Amerika, da kannst du in so eine Nische reingehen und woanders hinschieben.

T3: Aber Menschen wurden immer schon…

T6: Deine These ist also in Deutschland würde das nicht passieren?

T3: Ich glaube, dass es genauso passieren würde.

T4: Ich glaube auch, aber viel eher wenn du die amerikanische Kultur anguckst, viel eher in Amerika, viel eher in den großen Zentren, wo die Leute auf Begeisterung stehen, wo du sie viel leichter beeinflussen kannst.

T3: Aber Menschen wurden schon immer beeinflusst, das ist zwar heute größer durch die Technologie, aber PR und Propaganda, Hitler, das war auch Deutschland, das waren

auch unsere Großeltern. Die sind da genauso hinterher gelaufen, die wurden genauso beeinflusst, manipuliert oder was auch immer. Die Dimension ist nur heute einen andere, weil es global ist. Es ist nicht mehr so, dass die Städte plakatiert werden und da Leute auf Bühnen stehen und Reden halten, wo alle zuhören. Durch das Internet und die Technologie ist die Reichweite eine ganz andere. Die Menschen haben mehr Erfahrung. Du kannst viel besser, viel psychologischer detaillierter rangehen, aber von der Idee ist das dasselbe wie früher.

T4: Das denke ich auch, dass das dasselbe ist.

T1: Ist für mich ein kritischer Punkt. Also ich finde es richtig, dass das schon immer so passiert. Der Marktschreier versucht die Leute zum Kauf seiner Fische bewegen, in der Politik muss man reden können, aber was ich schon vom Gefühl her sagen würde und vielleicht reden wir auch deswegen darüber, und es wird generell viel darüber geredet. Es ist schon ein gruseliger Punkt, nicht dass im Marketing E-Mails an hunderte Adressen rausgeschickt werden und vielleicht guckt sich das einer an, also Spam Mails, hin zu wir analysieren Bevölkerungsgruppen, und gucken wofür sind die empfänglich, da auch mit Hass und Emotionen zu arbeiten, die im Internet momentan viel zur Geltung kommen. Negative Emotionen speziell zu nutzen von Leuten ,wo man vorher durch so eine unfassbar Analyse von Daten, die in einer großen Menge vorhanden sind, hat man wahnsinnig präzise Daten, das man solche Sachen vorhersehen und sagen kann, angewandte Philosophie an den Leuten zu praktizieren durch das Internet, das ist schon gruselig und das wird hoffentlich auch mal in die andere Richtung schwenken. Da ist jetzt die Datenanalyse gerade sehr stark, und man kann sehr nah ran an die Leute, vielleicht kommt jetzt über solche Regularien wieder etwas Ordnung rein.

Moderator: Ich muss jetzt einmal kurz zwischengrätschen, das ist bisher sehr gut gelaufen, auch das ihr Instrumentalisierung von Nutzer angesprochen habt, was für Gefahren es gibt. Der Nutzer kann ja nicht so viel dagegen tun, oder er kann es doch, tut es aber nicht, habt ihr ja auch bereits angesprochen. Ein frage die vielleicht auch kürzer zu beantworten ist: Willigt ihr regelmäßig bei COnsent-Verfahren, also Einwilligungsverfahren auf Websites ein, ohne die Datenschutzrichtlinien zum Beispiel zu lesen und mitgelieferte Informationen über das Tracking von Cookies oder Pixeln wahrzunehmen? Oder klickt ihr immer ok.

T3: Ja.

T4: Immer.

T6: Immer ja.

T2: seit der DSGVO nicht mehr.

T1: Ich würde sagen zwei unterschiedliche Sachen gibt es, bei Cookies gibt es ja nur OK. Wo ich mich frage wo ist da jetzt der Sinn, wenn ich auf OK drücke oder nichts mache, funktioniert die Website genauso, aber ich muss es mal gesehen haben.

T2: Seit der DSGVO kann man aber auch auf weitere Infos klicken und da macht es richtig Spaß alles auszumachen, Tracking aus, Personalisierte Werbung aus, aus, aus, aus. Wir dürfen Zugriff auf dein Gerät ist bei manchen Websites ganz oben, da mache ich immer alles aus.

T3: Das kommt bei mir gar nicht.

T2: Es muss kommen das ist verpflichtend.

T1: Ich mache immer alles aus was man auch machen kann.

T3: Dann habe ich das schon einmal weggeklickt.

T4: Da gibt es zwei Sachen, entweder du drückst bestätigen oder weitere Infos.

T2: Aber du musst von der Homepage in 2 Klicks zur DSGVO kommen.

T3: aber Homepage heißt dann bmw.de und wenn ich auf mercedes.de komme, dann muss das wiederkommen.

T2: Genau, wenn du auf BMW.de gehst, klickst du auf Impressum und dann Datenschutz, das muss in 2 Klicks erreichbar sein und dann kannst du da sowas einstellen.

T3: Aber du musst aktiv dahingehen?

T2: Ja, 2 oder 3 Klicks.

T3: Es poppt nicht auf?

T2: Doch es poppt beim ersten mal auf, müssen sie, denn sie wollen ja deine Daten benutzen und die meisten Leute klicken OK und weg. Baer du musst es auch wieder in 2 Klicks erreichen können, um es zu ändern. Sie dürfen es nicht so machen, ok du hast einmal OK gedrückt, die meisten Leute klicken auch bei den meisten Lizenzvereinbarungen ja gelesen.

T6: Also ich klick einfach immer ok.

Moderator: Ja ist in der Tat noch ein wenig Auslegungssache, wie das auch umgesetzt wird. Das ist nicht nur durch das Gesetz so gegeben, sondern mache Unternehmen machen das auch selbst proaktiv, setzen das in eigener Sache um. Was auch Teil der DSGVO ist, sind Betroffenenrecht, Die gab es ja zum Teil auch vorher schon. Recht auf Löschung, Recht auf Auskunft, Recht auf die Korrektheit von Daten, dass die nur aktuelle sein dürfen, nicht zu alte Daten gespeichert werden dürfen. Würdet ihr generell, einfach mal so gefragt, eure Daten anfragen, löschen oder berichtigen lassen?

T4: Ja

T6: Ich würde es tun weil es mich interessiert

T4: Einfach was die gesammelt haben von mir, das würde ich gerne wissen, was hat Google von mir

T6: Besonders Google würde mich interessieren

T4: Die haben sicher ein tierisches Profil von mir

T2: Das sind mehrere GB Textdaten, ich kenne mehrere die das gemacht haben.

T6: Ne das kriegst du von Google für dich lesbar, nicht irgendwelche kryptischen Ziffern

T2: Das ist ja nur ein Text im Endeffekt, und dann GB, das sind unfassbar viele Daten
T1: Ich würde zum Beispiel mal Löschen, wenn ich von Facebook weggehe. Dann würde ich sagen, so haut jetzt mal meine Daten raus und speichert nicht noch die siebte Kopie von meinem Profil.
T3: Kann man das machen?
T2: Ja kann man.
Moderator: Habt ihr irgendwelche dieser Betroffenenrechte schon mal in Anspruch genommen? Daten irgendwo angefragt, löschen oder berichtigen lassen?
- Kollektives Nein –
Moderator: Würdet es aber in Zukunft machen?
T4: Ich habe meinen Facebook Account schon mal so gelöscht, dass man ihn nicht reaktivieren kann.
T1: Da weiß man aber, da löscht es Facebook nicht, da heben sie die Daten eingefroren.
T2: Da sind wir wieder ein bisschen am Anfang. Bei Google. Da würde ich Daten nie anfragen, weil ich weiß nach 10 Suchanfragen, hat mich Google schon wieder katalogisiert, es würde sich gar nicht lohnen, die Daten zu löschen, ich benutze es sowieso. Die wissen sowieso alles. Was anderes wenn ich mein Facebook lösche, dann sollen sie auch alle Bilder löschen.
T4: Clean Cut, dass kannst du bei Google nicht machen, weil Google unumgänglich ist.
T2: Google ist aber auch eher so der Kumpel, während Facebook der nervige Nachbar ist.
T6: Wenn ihr euch mal googelt, da ist es schon verrückt was für Bilder und Verlinkungen da auftauchen.
T3: Bei mir ist da ganz logisch, Xing, Facebook und eine Sportseite wo mal über mich berichtet wurde. Ich kann alles nachvollziehen
T2: Bei mir kommt nichts.
T4: Bei mir auch nicht.
T1: auch nicht
Moderator: Würdet ihr für verstärkten Datenschutz auch zahlen in gewisser Weise? Also dann Facebook nutzen wo ihr keine Werbung bekommt, also eine Premium Version nutzen. Oder Abstriche machen was die User Experience angeht, also wenn ihr auf eine Website geht, nicht mehr getrackt wird, dafür aber auch nicht alle Inhalte sehen könnt, weil das Monetarisierungsmodell ja in gewisser Weise wegbricht?
Wäret ihr dazu bereit?
T3: Also Nein und Nein würde ich sagen.
T1: Also Facebook auf jeden Fall nein, würde ich niemals benutzen wenn es was kosten würde. Bei anderen Sachen. Also das wäre ja verrückt entweder wir verwenden deine Daten oder du zahlst Geld dafür, dass wir es nicht tun.

T2: Also finde ich jetzt nicht, es ist ja ein Unternehmen, das muss Geld verdienen, die müssen ihre Mitarbeiter bezahlen, wie wollen die das machen. In dem sie meine Daten verkaufen.

T6: Die verdienen ja alle Geld durch Werbung.

T2: Genau und das muss ja irgendwo herkommen, entweder man muss zahlen, dann nutzen sie die Daten nicht, dann werden sie konstant gelöscht, also ich finde es sind zwei ganz unterschiedliche Punkte. Wenn deiner UX eingeschränkt wird, wenn du deine Daten nicht nutzen lässt, dann funktioniert das ganze Konzept nicht mehr, dann strömen die Nutzer direkt weiter zur nächsten Plattform, das ist das Ende der Plattform.

T4: So ist es bei mir auch, wenn der AdBlocker aufpoppt, bitte deaktivieren sie den AdBlocker auf irgendeiner Sportseite, dann gehe ich auf eine andere Seite.

T6: Das Problem ist, dass wir alle Apps nutzen die kostenlos sind und dann nehme ich in Kauf, dass sie Werbung schalten. Entweder ich zaShle oder ich kriege Werbung. Das ist mir ja bewusst, dass sie Geld verdienen müssen. Und das ist ja schon eine Abwägung, wenn ich das nutzen will, muss ich auch dafür bezahlen.

T2: Ich würde sagen, was zu bezahlen, dass sie meine Daten nicht benutzen ist nicht das gleiche, wie dafür zu bezahlen, dass ich keine Werbung bekomme. Da habe ich einen AdBlocker, der ist umsonst. Oder ich benutze einen Browser, der eh alles blockt und nicht zulässt.

Moderator: Aber da funktioniert ja theoretisch eine Website nicht wirklich.

T2: Doch kann funktionieren.

Moderator: Kann aber auch als marktineffiziente Lösung angesehen werden.

T2: Natürlich, ist auch alles viel langsamer dann. Aber wenn man Wert darauf legt und sogar dafür bezahlt, dass sie Daten nicht verwenden oder eine Garantie aber dann kommt über einen Leak oder so raus, die benutzen es doch, dann hättest du ja schon mal rechtlich was in der Hand. Das finde ich viel besser als so ein Premium bei einer App, damit du nicht mehr Werbung siehst. Die Werbung guck ich mir an in meinen Apps, auf dem Handy habe ich keinen AdBlocker und nix, da ist es egal. Aber dafür zu zahlen, dass sie meine Daten nicht benutzen, finde ich interessanter, als dafür zu zahlen keine Werbung mehr zu sehen.

T1: Ich finde eigentlich dieses ganze System muss weg, riesige Konglomerate, die massiv Daten sammeln, um sie zu verkaufen.

T4: Das Ursprungsproblem ist, dass die Unternehmen damit so viel Geld verdienen, Werbung zu schalten.

T1: Das einzige wo man wirklich hin gehen kann, ist das jeder seine Daten selber verwaltet, nur so kann man einen Überblick darüber behalten. Dann muss man so viel wie möglich bei den Nutzern selbst lassen. Und wenn man Facebook oder andere Unternehmen als Mittelsmann hat, dann hat man keine Kontrolle mehr. Und ich finde, dass

das ganze Modell ein Auslaufmodell ist, und das Facebook in der Form nicht mehr lange da ist, ich finde das ist kein Modell der Zukunft, das ist teilweise zu böse.

T5: Man muss auch wieder den Vergleich haben, zwischen wir wollen immer neue Apps und Technologien, die uns das Leben vereinfachen und die müssen auch gefüttert werden mit Daten. Und was auch immer mehr im Kommen ist, ist die Sprachsteuerung. Bei Amazon, dass du da ordern kannst. Ich glaube schon, dass es in Zukunft noch viel mehr über Sprachsteuerung geht, oder der Kühlschrank selber bestellen kann, aber da brauch er auch wieder Daten, und wenn du diesen Luxus haben willst, dann müssen wir auch Daten abgeben.

T2: Ich habe das Präsentationsvideo von der neuen Google AI gesehen, da kansnt du einfach sagen Google buch mir einen Termin bei meinem Arzt, dann ruft die da an mit einer Computerstimme und bucht dir einen Termin, und der Typ am Telefon ahnt nicht mal, dass das eine AI ist, weil es so gut gemacht ist.

T6: Deswegen sage ich ja, zurück geht kein Weg mehr, weil man diesen Komfort schon so gewöhnt ist und nicht mehr drauf verzichten mag.

T3: Und du willst ja immer mehr.

T2: Ich finde nur von den Daten her, wenn man eine Datenspeicherung findet, die sicherer ist, ne Blockchain zum Beispiel. Es veralten die Daten auch total schnell, dein Wohnort, deine Interessen, für was du dich interessierst. Die Daten veralten irgendwann und in 5 Jahren sind sie nix mehr wert, weil man sich interessiert sich für was ganz anderes. Also ich glaube man kommt aus der Datenkrake schon raus, nicht deinen Namen und wo du mal zur Schule gegangen bist, aber alles was für Marketing interessant ist, ist ja das Aktuelle und nicht was einmal war. Nur die aktuellen Daten sind interessant, und die veralten, wenn es ein System gibt, in dem aktuelle Daten besser gespeichert werden.

Moderator: Dann kommen wir jetzt auch schon zum Ende, vielen Dank.

Eidesstattliche Erklärung

Ich, _____

geboren am _____

erkläre hiermit, die vorliegende Masterarbeit selbständig und ohne fremde Hilfe angefertigt zu haben. Dabei habe ich mich keiner anderen Hilfsmittel bedient als derjenigen, die im beigefügten Quellenverzeichnis genannt sind.

Alle Stellen, die wörtlich oder sinngemäß aus Veröffentlichungen entnommen wurden, sind von mir als solche kenntlich gemacht.

....., den …… ...……..

Studienort Unterschrift Studierende/r (= Verfasser/in)