WWU
MÜNSTER

Phänomene des Big-Data-Zeitalters

Eine rechtliche Bewertung im wirtschaftlichen und gesellschaftspolitischen Kontext

Thomas Hoeren (Hrsg.)

Thomas Hoeren (Hrsg.)

Phänomene des Big-Data-Zeitalters

WWU
MÜNSTER

Wissenschaftliche Schriften der WWU Münster

Reihe III

Band 35

Thomas Hoeren (Hrsg.)

Phänomene des Big-Data-Zeitalters

Eine rechtliche Bewertung im wirtschaftlichen und gesellschaftspolitischen Kontext

Wissenschaftliche Schriften der WWU Münster
herausgegeben von der Universitäts- und Landesbibliothek Münster
http://www.ulb.uni-muenster.de

Die Publikation wurde gefördert von dem Bundesministerium für Bildung und Forschung.

Bibliografische Information der Deutschen Nationalbibliothek:
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Dieses Buch steht gleichzeitig in einer elektronischen Version über den Publikations- und Archivierungsserver der WWU Münster zur Verfügung.
http://www.ulb.uni-muenster.de/wissenschaftliche-schriften

Thomas Hoeren (Hrsg.)
„Phänomene des Big-Data-Zeitalters. Eine rechtliche Bewertung im wirtschaftlichen und gesellschaftspolitischen Kontext“
Wissenschaftliche Schriften der WWU Münster, Reihe III, Band 35
Verlag readbox publishing GmbH – readbox unipress, Münster
http://unipress.readbox.net

ISBN 978-3-8405-0194-4 (Druckausgabe)
URN urn:nbn:de:hbz:6-96169492515 (elektronische Version)

direkt zur Online-Version:

Satz: Steffen Uphues
Umschlag: ULB Münster

Phänomene des Big-Data-Zeitalters[1]

–

Eine rechtliche Bewertung im wirtschaftlichen und gesellschaftspolitischen Kontext

Herausgegeben von:

Thomas Hoeren

Autoren:

Philip Bitter, Henning Brockmeyer, Nicolai Culik, Christian Döpke,
Lukas Forte, Tim Jülicher, Barbara Kolany-Raiser, Matthias Möller,
Maurice Niehoff, Tristan Radtke, Christian Straker, Tristan Julian Tillmann,
Steffen Uphues, Verena Vogt, Nils Wehkamp, Lucas Werner

1 Die Dossiers wurden im Rahmen des ABIDA-Projekts (Förderkennzeichen: 01|S15016A-F) mit Mitteln des Bundesministeriums für Bildung und Forschung erstellt. Der Inhalt der Dossiers gibt ausschließlich die Auffassungen der Autoren wieder. Diese decken sich nicht automatisch mit denen des Ministeriums oder der einzelnen Projektpartner.

Inhaltsübersicht

Inhaltsverzeichnis

Vorwort

Nehmen wir einmal an, ein Mann namens Marten sucht auf der Online-Plattform Amazon nach einer neuen Hose für den bevorstehenden Sommer. Nach längerem Suchen wird er fündig und entscheidet sich für eine schmal geschnittene Leinenhose aus dünnem Stoff. Nachdem er den Artikel seinem Warenkorb hinzugefügt hat, erscheint unter der Überschrift „Kunden, die diesen Artikel gekauft haben, kauften auch…“ ein Hinweis auf Chelsea Boots. Marten, der sich bislang nicht viel mit Mode-Trends befasst hat, wird neugierig und klickt auf die Schuhe, um mehr über sie zu erfahren. Nach Ansicht der Bilder und der Produktinformationen ist er von diesen begeistert und bestellt sogleich Leinenhose und Schuhe. Die Anzeige der Schuhe erfolgte, da Amazon durch Algorithmen sämtliche Bestelldaten in höchster Geschwindigkeit verarbeiten lässt und hierdurch Muster erkennen kann, etwa welche Kleidungsstücke oftmals in Kombination gekauft werden. Damit solch ein Algorithmus aussagekräftige Ergebnisse präsentieren kann, benötigt man eine Vielzahl an Daten, aus denen sich ein Muster erkennen lässt – man benötigt Big Data. Selbstlernende Algorithmen können in der Folge darüber hinaus Trendverschiebungen in ihre Analysen miteinfließen lassen. Sollte sich die Mode dahingehend wandeln, dass Leinenhosen auf den Laufstegen dieser Welt zukünftig mit Skateschuhen präsentiert werden, könnten Algorithmen darauf basierende Kaufentwicklungen erkennen und würden ab einer gewissen Anzahl kombinierter Einkäufe im obigen Beispiel Skateschuhe zur Leinenhose empfehlen – Kaufberatung durch Künstliche Intelligenz. Eben diese Künstliche Intelligenz wird darüber hinaus auch eingesetzt, um etwa die logistische Planung in einem Unternehmen wie Amazon zu steuern. Wird etwa eine ansteigende Nachfrage an Leinenhosen registriert, so werden automatisch frühzeitig weitere Exemplare geordert, um diese stets vorrätig zu haben und sie dem Kunden nach einem Kauf auf dem von Algorithmen erfassten schnellsten Weg zu liefern – herzlich Willkommen in der Industrie 4.0.

Big Data ist zurzeit – ähnlich wie *Industrie 4.0* oder auch *Künstliche Intelligenz* – ein beliebtes Schlagwort auf wissenschaftlichem sowie gesell-

schaftlichem Parkett. Wichtig ist hierbei, diese Begriffe in einem einheitlichen Kontext zu behandeln und nicht etwa gegeneinander abzugrenzen. Das oben ausgeführte Beispiel macht deutlich, dass alle drei Begriffe nur einer groben Einordnung von Sachverhalten dienen. Darüber hinaus gab es bereits zuvor industrielle Revolutionen und es gab den Begriff der Künstlichen Intelligenz schon in den 50er Jahren. Der Begriff Big Data, zu dem es keine einheitliche Definition gibt und dem sinnvollerweise auch keine abschließende Definition zuteilwerden sollte, ist immer von einem technischen Blickwinkel aus zu bestimmen. Big Data meint nichts anderes als einen Zustand, in dem die vorhandene Datenmenge so groß ist, dass sie mit den zur Datenverarbeitung vorhandenen Mitteln nicht in dem bislang üblichen Zeitraum und nicht mit den bislang hierfür eingesetzten Systemen bzw. Algorithmen analysiert werden kann – insofern ist Big Data keine neue Entwicklung.

Es gilt, sich auf die Besonderheiten zu konzentrieren, welche die momentane Situation kennzeichnen: Immer mehr Dienste funktionieren digital und können miteinander vernetzt werden. Dabei werden immer häufiger bisher bilaterale Verhältnisse aufgebrochen und es entstehen Mehrparteienverhältnisse, in denen etwa die Frage nach Datenzuordnung oder die Frage nach möglichen Anspruchsgegnern an Komplexität gewinnt. Der durchschnittliche Internetnutzer kommt heutzutage nicht drum herum, digitale Plattformen zu nutzen, wobei aufgrund von direkten und indirekten Netzwerkeffekten häufig einige wenige hiervon eine mächtige Marktstellung innehaben und darüber diskutiert werden kann, ob dem Nutzer faktisch überhaupt eine Wahlmöglichkeit bezüglich des Diensteanbieters verbleibt. Ein weiterer Fokus liegt auf den Intermediären, welche im Bereich der Finanzen oder auch der Meinungsbildung eine gewichtige Rolle einnehmen. Daneben bestehen immer vielfältigere Möglichkeiten, Daten abzugreifen bzw. zu teilen, sodass – auch aufgrund der Tatsache, dass immer größere Speicherkapazitäten vorhanden sind – einmal „in das Internet eingepflegte“ Daten nur schwer wieder gelöscht werden können, ohne dass diese bereits dupliziert wurden und somit an anderer Stelle noch vorhanden sind.

Einigen zurzeit relevanten Fragestellungen zu Aspekten rund um Big Data widmet sich dieser Sammelband. Er setzt sich zusammen aus einzelnen Dossiers, welche im Rahmen des ABIDA-Projekts verfasst wurden und sich mit Problemen spezifischer Lebensbereiche befassen.

Das ABIDA-Projekt wird vom Bundesministerium für Bildung und Forschung finanziert und forscht seit dem Frühjahr 2015 zu den gesellschaftlichen Auswirkungen des Einsatzes von Big-Data-Anwendungen. Hierzu befassen sich Forschungsstellen mit rechtlichen (Leibniz Universität Hannover), politikwissenschaftlichen (Wissenschaftszentrum Berlin für Sozialforschung), soziologischen (Technische Universität Dortmund), ethischen (Karlsruher Institut für Technologie) sowie ökonomischen (Ludwig-Maximilians-Universität München) Implikationen von Big Data. Das Projekt wird geleitet vom Institut für Informations-, Telekommunikations- und Medienrecht (Münster) sowie dem Institut für Technikfolgenabschätzung und Systemanalyse (Karlsruhe).

Die vorliegenden Dossiers behandeln zunächst (gesellschafts-)politische Themen (A.-G.), bevor anschließend auf einzelne Fragestellungen spezifischer Lebensbereiche wie etwa dem Versicherungswesen (H.) oder dem Finanzwesen (J.) eingegangen wird. Inhaltlich liegt der Fokus dabei auf rechtlichen Gesichtspunkten, die je nach Dossier um ökonomische, soziologische, politologische oder ethische Implikationen ergänzt werden.

Münster, im Januar 2019

Prof. Dr. Thomas Hoeren

A. Big Data for Policy Making – Herausforderungen algorithmischer Politikgestaltung (Tim Jülicher)

Stand: September 2017

Abstract: Big Data for Policy Making

Während die Implementierung von Big-Data-Technologien im privaten Sektor zügig voranschreitet, wirkt der öffentliche Sektor weitaus zurückhaltender. Obwohl Beispiele aus der Praxis auf ein großes Innovationspotential hindeuten, konnte sich die Technologie bislang nicht etablieren. Diese Beobachtung nimmt der Beitrag zum Anlass, Big Data Analytics als Hilfsmittel für Policy Maker zu untersuchen und limitierende Faktoren eines umfassenderen Einsatzes aufzuzeigen.

I. Einleitung

Big-Data-Technologien haben ihren Ursprung in der Privatwirtschaft, doch längst hat das Versprechen datengestützter algorithmischer Optimierung auch den öffentlichen Sektor ergriffen. Zahlreiche Beispiele der vergangenen Jahre nähren die Hoffnung, dass Big Data Analytics den Akteuren des politischen Systems ein neues Werkzeug liefert, um Policies evidenzbasiert am gesellschaftlichen Nutzen auszurichten:

Beispiel I: Big Data for Development (BD4D)

Mit der Initiative „UN Global Pulse“ etablierten die Vereinten Nationen 2009 eine Plattform, die sich dem Einsatz von Big-Data-Technologien zum Zwecke der Entwicklungshilfe und zur Bewältigung humanitärer Katastrophen verschrieben hat. Dabei sind die Anwendungsszenarien denkbar vielfältig: Im Nachgang des Nepal-Erdbebens (2015) fand beispielsweise eine anonymisierte Echtzeitanalyse der Mobilfunkdaten

von 12 Millionen Menschen statt, um die Verteilung von Hilfsgütern und -kräften bestmöglich auf die Bewegungsmuster der Bevölkerung abzustimmen.[2] In anderen Fällen wurden Inhalte sozialer Netzwerke analysiert, um die Preisentwicklung von Nahrungsmitteln[3] oder die Akzeptanz von Impfungen[4] zu evaluieren. Auch bei der Bekämpfung der Ebola-Epidemie kamen Big-Data-Technologien zum Einsatz, um internationale, nationale und regionale Akteure im *Disease Management* zu unterstützen.

Beispiel II: Urbane Entwicklung

Unter dem Schlagwort „Smart City" wird seit gut einem Jahrzehnt die Idee einer ubiquitären Vernetzung des urbanen Raums forciert.[5] In Metropolen wie Rio de Janeiro, London oder New York laufen vielfältige Datenströme in städtischen Kommandozentralen zusammen, wo sie in Echtzeit verarbeitet, analysiert und visualisiert werden, um etwa die Luftverschmutzung zu bekämpfen, Anwohnern die Parkplatzsuche zu erleichtern, Ordnungs- und Rettungskräfte zu unterstützen oder eine prognosebasierte Kriminalitätsbekämpfung (Predictive Policing) zu ermöglichen. Die Vision einer „Smart City" verspricht Sicherheit, Effizienz und Nachhaltigkeit.[6] Dabei werden die zur Umsetzung dieser Ziele benötigten Daten von unzähligen Sensoren in Smartphones, Fahrzeugen, Mülleimern, Ampeln oder Straßenlaternen gesammelt. In der südchinesischen Provinz Fujian wurden dazu jüngst 120.000 öffentliche Verkehrsmittel mit GPS-Sendern ausgestattet. Deren Datenstrom wird – angereichert mit Videomaterial aus der Verkehrsüberwachung – kontinuierlich analysiert, um eine dynamische Verkehrssteuerung zu erzielen und so dem allgegenwärtigen Verkehrschaos zu begegnen.[7] Vergleichbare (Pilot-)Projekte gibt es auch in Europa, etwa in der nordspanischen Stadt Santander.

---

2 UN Global Pulse, The State of Mobile Data for Social Good Report, S. 7.

3 UN Global Pulse, Mining Indonesian Tweets to Understand Food Price Crises.

4 UN Global Pulse, Understanding Public Perceptions of Immunisation Using Social Media.

5 Ausführlich Kitchin, Big Data & Society 2014, 1, 1 ff.

6 DIVSI, S. 3.

7 Dell, S. 3.

Die beiden Beispiele zeigen, welch verheißungsvolles Potential Big Data im Bereich Policy Making zugeschrieben wird. Jedoch täuscht das diskursive Framing schnell darüber hinweg, dass es sich vielfach nur um Pilotprojekte exemplarischer Natur handelt und von einer flächendeckenden Implementierung noch lange keine Rede sein kann.

Für eine kritische Beurteilung des tatsächlichen Innovationspotentials der Technologie stellt sich daher – nicht nur für Policy Maker, sondern für alle Stakeholder – die Frage, welche theoretischen und praktischen Hindernisse ihr entgegenstehen. Um dies herauszufinden, wird im Folgenden zunächst auf den Big-Data-Begriff im Policy-Kontext (II.), relevante Politikfelder (III.) sowie das Policy-Cycle-Modell (IV.) eingegangen. Anschließend werden das Innovationspotential (V.) und limitierende Faktoren (VI.) beleuchtet.

II. Begriffliche Abgrenzung

1. Defizite der gängigen Big-Data-Definitionen

Big Data wird üblicherweise mithilfe der drei Merkmale *Volume* (Datenmenge), *Variety* (Heterogenität der Daten) und *Velocity* (Geschwindigkeit der Datenverarbeitung) beschrieben. Da diese Definition jedoch an die Phänomenologie privatwirtschaftlicher Anwendungsszenarien von Big Data knüpft, lässt sie sich nur eingeschränkt für den politischen Kontext operationalisieren.

So kann in Zweifel gezogen werden, ob amtliche Datenbestände eine hinreichende Heterogenität aufweisen[8], wenn sie doch regelmäßig strukturierter Natur sind (etwa im Fall von Akten oder Formularen). Da sich aus der Kontextabhängigkeit der jeweiligen Datenbestände und -quellen aber ein beachtliches Maß an *Variety* ergeben kann, greift der Einwand zu kurz:[9] Man denke nur an die Datenheterogenität innerhalb einer Behörde (z.B. ermittlungsbehördliches Audio-, Foto- und Textmaterial) oder

---

8 Malomo/Sena, Policy & Internet 9(1), 7, 11.

9 Malomo/Sena, Policy & Internet 9(1), 7, 11.

die behördenübergreifende Zusammenführung von Daten (z.B. Metadaten der Verkehrssteuerung einerseits und steuerstrafrechtliche Ermittlungsakten andererseits).

Vor dem Hintergrund dieser besonderen Daten- und Quellenvielfalt wird die Definition der „3 Vs“ im politisch-administrativen Kontext vielfach um ein weiteres Charakteristikum – nämlich das Merkmal der *Komplexität* – ergänzt, wodurch gezielt den spezifischen Herausforderungen eines behörden-, ebenen- und gewaltenübergreifenden Informationsaustauschs Rechnung getragen werden soll.[10]

2. Abgrenzung zu anderen Konzepten

Der Big-Data-Begriff ist keineswegs trennscharf, sondern bedarf – gerade im Policy-Kontext – einer Abgrenzung zu verwandten Begriffen und Konzepten, namentlich Open Data, Open Knowledge und Open Government.

- Unter **Open Data** werden Daten verstanden, die „durch jedermann und für jegliche Zwecke genutzt, weiterverarbeitet und weiterverbreitet werden können“.[11]
- Ein ganz ähnliches Konzept liegt **Open Knowledge** zugrunde. Wissen wird hier als Oberbegriff verstanden, der auch – aber eben nicht nur – Daten umfasst. Wissen ist frei „wenn jeder darauf frei zugreifen, es nutzen, verändern und teilen kann – eingeschränkt höchstens durch Maßnahmen, die Ursprung und Offenheit des Wissens bewahren“.[12]
- In beiden Fällen geht es regelmäßig um den Zugang zu Informationen, die sich in staatlicher Hand befinden und Bürgerinnen und Bürgern nicht per se zugänglich sind. Angesichts dieser Informationsasymmetrie ist das Ziel der **Open-Government**-Bewegung, die betreffenden Behörden, Gerichte und Parlamente zu verpflichten, möglichst viele dieser Daten im Interesse von Transparenz und Partizipation *by default* zur Verfügung zu stellen. Für zivilgesellschaftliche Kollektiv-

---

10 Malomo/Sena, Policy & Internet 9(1), 7, 8 ff.

11 Dietrich, Was sind offene Daten?

12 So die Zusammenfassung der sog. Open Definition 2.0, abrufbar unter http://opendefinition.org/od/2.0/de/ (zuletzt abgerufen: 11/2018).

und Individualakteure stellt insoweit der in den Informationsfreiheitsgesetzen des Bundes und der Länder normierte Anspruch auf Informationszugang ein wichtiges Instrument dar (*freedom of information*); ein bundesdeutsches Open-Data-Gesetz wurde im Sommer 2017 verabschiedet. Zugleich haben viele Staaten zentrale Plattformen eingerichtet, über die sie Daten zur Verfügung stellen (z.B. govdata.de, data.gov oder data.gov.uk).

Offene Daten sind sowohl für nichtstaatliche Akteure (NGOs, MNCs, Bürgerinnen und Bürger) als auch für andere staatliche Akteure (etwa benachbarte Kommunen, Aufsichtsbehörden oder supranationale Institutionen) eine wertvolle Informationsquelle, die ihrerseits als Teil einer Big-Data-Anwendung zum Zweck datengestützten Policy Makings genutzt werden kann. Big Data und Open Data schließen einander somit keinesfalls aus, sondern weisen – je nach Kontext – weitreichende Überschneidungen auf.

III. Relevante Politikfelder

Welche Politikfelder kommen für den Einsatz von Big-Data-Technologien in Betracht? Da vielfältige Anwendungsszenarien denkbar sind, erhebt die nachfolgende Übersicht keinen Anspruch auf Vollständigkeit:

- **Verkehrspolitik** (z.B. Realisierung einer datenbasierten Verkehrsstromanalyse und -planung, Modellierung von Emissionen, Energieeffizienzsteigerungen, Optimierung der ÖPNV-Auslastung)
- **Finanz- und Wirtschaftspolitik** (z.B. präventive Finanzmarktaufsicht, Effizienzsteigerungen in Finanzverwaltung und Wirtschaftsförderung)
- **Bildungspolitik** (z.B. Educational Data Mining, Learning Analytics, Benchmarking von Bildungseinrichtungen[13])
- **Arbeitspolitik** (z.B. verbesserte Prognosen und Szenarioanalysen des Arbeitsmarktes)
- **Entwicklungspolitik** (z.B. Krisenbewältigung, Disease Control, Ressourcenallokation)

---

[13] Zum Thema Big Data und Bildung siehe Jülicher, in: Hoeren/Kolany-Raiser (Hrsg.), Big Data zwischen Kausalität und Korrelation, S. 55-62.

- **Innen- und Sicherheitspolitik** (z.B. Predictive Policing, Terrorismusbekämpfung, Cyber Security)[14]
- **Gesundheitspolitik** (z.B. Epidemiologie, Vernetzung von Akteuren, medizinische Forschung); Länder wie Kanada schlossen sich unter dem Druck der EU mit dem PIPEDA Act im Jahr 2000 den dortigen Grundsätzen der Datenqualität an.

IV. Big Data im Policy Cycle

In der politikwissenschaftlichen Forschung existieren verschiedene Modelle, um den Prozess des Policy Makings abzubilden und zu analysieren. Der insoweit wohl prominenteste Ansatz stammt vom Psychologen und Politikwissenschaftler *Harold Lasswell*, der von einem idealtypischen Politikzyklus, dem sog. Policy Cycle, ausgeht.

Am Anfang des Lasswell'schen Policy Cycle steht das Erkennen und Definieren eines politischen Problems (**Problemdefinition**). Politische und gesellschaftliche Akteure versuchen anschließend, das Thema auf die politische Agenda zu bringen (**Agenda Setting**) und Policies zur Problemlösung zu formulieren (**Politikformulierung**). Es schließt sich die Phase der Policy-**Implementierung** an, bevor im Zuge einer **Evaluierung** über die schlussendliche Neuformulierung oder **Terminierung** der Politik entschieden wird.[15]

In all diesen Phasen kommt der Einsatz von Big-Data-Technologien in Betracht.[16] Mit ihrer Hilfe lassen sich zunächst Korrelationen und Muster in vorhandenen Datenbeständen identifizieren, um politische Probleme zu definieren.[17] Im Zuge des Agenda Settings können soziale Netzwerke und Onlinemedien instrumentalisiert werden, um einem Thema die gewünschte Aufmerksamkeit zu verschaffen und den öffentlichen Diskurs im eigenen Interesse zu beeinflussen. Für die Phase der Politikformulierung lassen sich algorithmische Vorhersagen (sog. Predictive Analytics)

---

14 Jülicher, ADLAS 1/2016, S. 14 ff.

15 Ausführlich Blum/Schubert, S. 104 ff.

16 Deloitte, S. 11; Mureddu et al., S. 62, 65.

17 Poel et al., S. 81.

und datengestützte Szenario-Modelle fruchtbar machen.[18] Sie erlauben es insbesondere, Alternativen und Machbarkeiten abzuschätzen. In der Implementierungsphase angelangt, können mithilfe von Big Data Analytics prioritäre Einsatzbereiche abgesteckt werden. Und in der Evaluierungsphase besteht schließlich die Möglichkeit eines kontinuierlichen Echtzeit-Feedbacks, mithilfe dessen die Policy-Evaluierung nicht erst nach Abschluss, sondern schon während der Implementierungsphase ansetzen kann.[19]

V. Innovationspotential für Policy Making

Die zentralen Versprechen hinsichtlich des Innovationspotentials von Big Data für den Policy-Making-Prozess lassen sich wie folgt skizzieren:

- Als zentrales Argument für eine umfassende Implementierung von Big-Data-Technologien werden **Kosteneinsparungen und administrative Effizienzsteigerungen** ins Feld geführt. So beziffert die Unternehmensberatung McKinsey das Einsparungspotential im öffentlichen Sektor allein für die Verwaltung der Europäischen Union auf bis zu 250 Milliarden Euro.[20] Als Blaupause für die Evaluierung und Optimierung öffentlicher Services dienen privatwirtschaftliche Unternehmen, die mithilfe von Big Data Analytics signifikante Produktivitätssteigerungen realisieren konnten. Unter Effizienzgesichtspunkten könnten grundsätzlich alle Phasen des Policy Cycles profitieren.
- Als Instrument evidenzbasierter Politikgestaltung erwecken Big-Data-Technologien – wie alle Ansätze zur „Verwissenschaftlichung“ politscher Entscheidungsfindung – den Anschein technischer **Objektivität, Akkuratesse und Rationalität**. Das klassische Narrativ lautet: Sobald es genug Daten gibt, sprechen diese für sich selbst.[21] Dadurch

---

18 Höchtl et al., Journal of Organizational Computing and Electronic Commerce, 26(1-2), S. 135, 160.

19 Höchtl et al., Journal of Organizational Computing and Electronic Commerce, 26(1-2), S. 135, 162.

20 Henke et al., S. 29.

21 Anderson, The End of Theory.

wird – gerade in den Zyklusphasen der Politikformulierung und -implementierung – eine absolute Überlegenheit algorithmischen Decision Makings suggeriert.

- Ferner versprechen Big-Data-Technologien, Policy Making durch die Bereitstellung und Auswertung von Informationen in **Echtzeit** zu unterstützen.[22] Hilfreich dürfte dies vor allem in den Phasen der Formulierung und Evaluierung von Policies sowie in Politikfeldern sein, die nach einem raschen Handeln politischer Akteure verlangen (etwa in der Entwicklungs- oder Sicherheitspolitik). Es ist auch denkbar, dass verantwortliche Policy Maker durch Big-Data-Technologien zu einem schnelleren Agieren motiviert werden. In der Vergangenheit gelang dies etwa im Bereich der Krisenbewältigung erfolgreich. So motivierten sog. Crowdsourcing-Plattformen, auf denen sich freiwillige Helferinnen und Helfer (*Crisis Mapper*) zusammenschlossen, um nach Naturkatastrophen die Aufenthaltsorte Betroffener zu bestimmen, staatliche Stellen zu einer zügigen Krisenbewältigung.
- Klassischerweise ist das Handeln politischer Akteure auf die ex-post-Bewältigung vorhandener Probleme gerichtet, d.h. retrospektiver Natur. Demgegenüber eröffnen wahrscheinlichkeitsbasierte Big-Data-Prognosen ein an künftigen Herausforderungen orientiertes, proaktives Handeln.[23] Probleme lassen sich also in einem besonders frühen Stadium erkennen und gezielt adressieren.[24] Diese Form eines **Probabilistic Policy Making** stellt eine neue Entscheidungsgrundlage und mithin einen alternativen Ansatz für Politiksetzungsprozesse dar.
- Last but not least befeuert Big Data im Zusammenspiel mit Open Data die Hoffnung auf eine **Öffnung des politischen Systems**. Nach dem Systemverständnis von *David Easton* ist das Zustandekommen von Policy-Entscheidungen – gemeint ist die Umsetzung von Inputs in Outputs – für Außenstehende nicht nachvollziehbar (sog. *Black Box*). So-

---

22 Höchtl et al., Journal of Organizational Computing and Electronic Commerce, 26(1-2), S.147, 149.

23 Malomo/Sena, Policy & Internet 9(1), S. 7, 9; Margetts, The Promises and Threats of Big Data for Public Policy-Making.

24 Mureddu et al., S. 62, 64.

wohl offene (Regierungs-)Daten, wie sie beispielsweise über Datenportale und offene Schnittstellen bereitgestellt werden, als auch die Objektivität algorithmischer Prozesse könnten dazu beitragen, staatliches Handeln transparenter und nachvollziehbarer zu machen und mehr Partizipationsmöglichkeiten zu eröffnen.

VI. Limitierende Faktoren

Trotz des beachtlichen Innovationspotentials ist Big Data für Policy Maker – anders als für Akteure in Wissenschaft und Privatwirtschaft – bislang eher eine theoretische Vision denn praktische Realität. Für dieses Implementierungsdefizit lassen sich verschiedene Faktoren identifizieren:

1. Kapazitätsdefizite

Das politisch-administrative System weist gegenüber dem privaten Sektor eine signifikant geringere IT-Affinität und Investitionsbereitschaft auf. Dies ist insofern problematisch, als die Digitalisierung nicht nur nach umfangreichen infrastrukturellen Investments, sondern auch nach besonderer Fachkompetenz verlangt. Um Big-Data-Technologien flächendeckend und sinnvoll einsetzen zu können, bedarf es qualifizierter Fachkräfte, die die Implementierung begleiten und vorantreiben. Unter kompetitiven Gesichtspunkten ist es für den öffentlichen Sektor essentiell, spezifische Aus- und Weiterbildungsmaßnahmen in den Fokus zu nehmen und die Attraktivität gegenüber privaten Arbeitgebern zu fördern.

2. Mangelnde Interoperabilität

Aus technischer Sicht fehlt es nicht nur an verbindlichen gemeinsamen Standards für den behördenübergreifenden Datenaustausch, sondern auch an geeigneten Schnittstellen zu außerhalb des politisch-administrativen Systems stehenden Dritten.[25] Gerade im Interesse eines erfolgreichen Zusammenwirkens der verschiedenen Stakeholder gilt es daher, Interoperabilität durch gezielte Maßnahmen wie etwa die Förderung offener

---

[25] Malomo/Sena, Policy & Internet 9(1), S. 7, 13.

Standards oder die Schaffung tauglicher Schnittstellen in proprietärer Software zu forcieren.[26]

3. Strukturelle Hürden

Nicht nur technisch, sondern auch organisatorisch-strukturell existieren beachtliche Hürden. So zeichnen sich Staat und Verwaltung traditionell durch eine starke organisationsrechtliche, insbesondere föderale Fragmentierung aus: Eine strikte Gewaltenteilung und klare Kompetenzzuweisungen in vertikaler wie horizontaler Hinsicht stehen einem systemweiten Informationsaustausch (*free flow of information*) – freilich aus guten Gründen – strikt entgegen. Infolgedessen haben Policy Maker immer nur Zugriff auf einen Bruchteil des Idealbestandes. Sie sind also stets auf die Zusammenarbeit mit anderen Akteuren und deren kooperatives Wohlwollen angewiesen. Abhilfe können punktuell-anwendungsbezogene Kooperationsmodelle zwischen Stakeholdern schaffen; etwa Netzwerke auf kommunaler Ebene zur Beantwortung lokaler Fragestellungen.[27]

4. Datenqualität

Für Big Data Analytics spielt die Qualität der verwendeten Daten eine maßgebliche Rolle.[28] Soll die Technologie für eine evidenzbasierte Unterstützung des Policy-Making-Prozesses genutzt werden, müssen die zugrundeliegenden Daten möglichst aktuell, vollständig, inhaltlich richtig und belastbar sein.[29] Gerade dies ist in der Realität aber zumeist nicht der Fall: Anders als soziale Netzwerke, die jede Aktivität ihrer Nutzerinnen und Nutzer speichern, analysieren und auswerten, stehen den Behörden in der Regel weitaus weniger aussagekräftige Informationen (z. B. Daten der Einwohnermeldeämter oder von Kfz-Registrierungen) zur Verfügung. *Victoria Nash* spricht daher von einer „fundamentalen Datenasymmetrie“, die im Interesse einer Verbesserung der Datenqualität nach einer

---

26 Deloitte, S. 97.

27 Malomo/Sena, Policy & Internet 9(1), S. 7 ff.

28 Hoeren, in: Ders./Kolany-Raiser (Hrsg.), Big Data zwischen Kausalität und Korrelation, S. 3-17.

29 Nash, Responsible research agendas for public policy in the era of big data.

Zusammenarbeit staatlicher Stellen verlange.[30] Diese Datenasymmetrie gibt es aber freilich auch unter Akteuren des privaten Sektors – man denke nur an den Wettbewerb zwischen stationärem Einzelhandel und Internethändlern. Ohnehin bliebe zu klären, ob und inwieweit eine von *Nash* geforderte sektor- und institutionenübergreifende Datenzusammenführung („*merged data*“) überhaupt praktikabel und wünschenswert wäre.

5. Materiellrechtliche Hürden

Eine Vielzahl von Regulierungsregimen setzt der tatsächlichen Ausweitung der Datensammlung, -auswertung und -analyse durch Big Data – vor allem in Bezug auf einen offenen und behördenübergreifenden Datenaustausch – rechtliche Schranken. Dazu zählt zuvörderst der besondere Schutz personenbezogener Daten durch das informationelle Selbstbestimmungsrecht. Neben dem Datenschutzrecht entfalten auch das Recht des geistigen Eigentums sowie der Schutz von Betriebs- und Geschäftsgeheimnissen limitierende Wirkung. Ferner haben staatliche Stellen untereinander sowie gegenüber Dritten ein berechtigtes Interesse an der Geheimhaltung der ihnen (womöglich exklusiv) zur Verfügung stehenden Informationen, soweit sie beispielsweise die innere Sicherheit, die Wettbewerbsregulierung oder militärische Belange berühren.

6. Epistemologische Grenzen

Da für die Auswertung großer Datenmengen mit Big Data Analytics statistische Berechnungen und Analyseverfahren eine zentrale Rolle spielen, sind mit Blick auf die Gewinnung politischer Handlungsempfehlungen eine Reihe von Überlegungen aus der Statistik in Rechnung zu stellen.

Dies gilt zunächst für die Auswertung der Analyseergebnisse: So vermag Big Data zwar Zusammenhänge zu identifizieren, aber keine kausalen Erklärungen zu liefern. Für eine fundierte Politikgestaltung ist deshalb stets ein hinreichendes Maß an Hintergrundwissen (*domain-specific knowledge*) notwendig.[31] Weil Daten aber auch im Zeitalter intelligenter

---

30 Nash, Responsible research agendas for public policy in the era of big data.

31 Kitchin, Big Data & Society 2014, S. 1, 4.

Algorithmen noch immer einer kontextabhängigen – und damit subjektiven – Dateninterpretation bedürfen, sprechen sie gerade nicht für sich selbst.[32] Ein Bias und/oder Framing kann daher auch mithilfe von Big Data nicht vollständig eliminiert werden.[33]

Darüber hinaus haben die Auswahl und der Umfang der herangezogenen Daten weitreichende Konsequenzen für die Aussagekraft und Belastbarkeit der Ergebnisse. Sie stellen für sich genommen nur einen kleinen Ausschnitt der Realität dar und vermögen infolgedessen nur mittelbare Anknüpfungspunkte für politische Problemlösungsstrategien zu liefern. Wie in allen Bereichen der Statistik gilt deshalb, dass ein Mehr an Daten nicht automatisch zu einem Mehr an Qualität führt.[34]

Ein elementares Problem ist schließlich, dass die zugrundeliegenden Daten unausweichlich vergangenheitsbezogen und damit hinsichtlich ihrer Vorhersagekraft – zumal im Fall dynamischer Umweltbedingungen – limitiert sind.[35]

7. Gesellschaftliche Implikationen

Zu guter Letzt wirft Big Data im Kontext von Politikgestaltungsprozessen eine Reihe gesellschaftlicher und ethischer Fragen auf.

Erstens droht dort, wo Entscheidungen ausschließlich oder überwiegend aufgrund wahrscheinlichkeitsbasierter Prognosen gefällt werden, staatliche Diskriminierung.[36] Je komplexer algorithmische Entscheidungen werden, desto mehr gewinnt aus diesem Grund die Gewährleistung von Transparenz, Rechtsstaatlichkeit und Demokratie an Bedeutung, denn ein datengestütztes, algorithmisches Policy Making läuft Gefahr, dystopische Ängste vor einer undurchschaubaren Technokratie hervorzurufen.[37]

---

32 Boyd/Crawford, Information, Communication & Society 15(5), S. 662, 666.

33 Kitchin, Big Data & Society 2014, S. 1, 5; Boyd/Crawford, Information, Communication & Society 15(5), S. 662, 667.

34 Boyd, Privacy and Publicity in the Context of Big Data; Boyd/Crawford, Information, Communication & Society 15(5), S. 662, 668.

35 Hilbert, Development Policy Review 34(1), S. 135, 163.

36 Malomo/Sena, Policy & Internet 9(1), S. 7, 15 f.

37 Helbig et al., Will Democracy Survive Big Data and Artificial Intelligence?.

Zweitens ruft die Kooperation staatlicher und privater Akteure Kritiker auf den Plan, die nicht nur Deregulierung und Privatisierung fürchten.[38] Indem IT-Unternehmen Hardware liefern, den Aufbau vernetzter Systeme unterstützen, Algorithmen entwickeln, technische Standards schaffen und Datenexpertinnen und -experten schulen, erweitern sie (in-)direkt ihren Einfluss auf das politische System. Im Zuge dessen drohen staatliche Akteure schnell in technologische Abhängigkeiten (sog. Lock-In-Effekt) zu verfallen.[39]

Drittens ist die gesellschaftliche Rezeption des Themas nicht zu unterschätzen: Big Data in den Händen des Staates – insbesondere der Sicherheitsbehörden und Geheimdienste – ist spätestens seit dem NSA-Skandal ein äußerst heikles Thema.[40] Jeder Einsatz von Big-Data-Technologien sollte daher den in der Bevölkerung verankerten Wunsch nach mehr Bildung zum Thema Big Data berücksichtigen und mit grundlegenden Aufklärungsmaßnahmen einhergehen.[41] Hierfür bieten etwa die Bundes- und Landeszentralen für politische Bildung geeignete Plattformen und Kanäle.

VII. Fazit

Big-Data-Technologien versprechen in nahezu allen Politikfeldern Verbesserungen für den öffentlichen Sektor sowie für Policy Maker. Da sich die Technologie jedoch einer Vielzahl von Hürden gegenübersieht, sollte sie in ihrem Innovationspotential nicht überschätzt werden.

Zu einer radikalen Transformation politischer Entscheidungsfindung wird es (auch) mit Big Data Analytics nicht kommen. Vielmehr handelt es sich um ein neues Werkzeug evidenzbasierter Politikgestaltung, das Policy Maker je nach Anwendungsfall ergänzend zum etablierten Instrumentarium heranziehen können. Als solches verlangt es nach einem umsichtigen und verantwortungsvollen Einsatz.

---

38 Kitchin, Big Data & Society 2014, S. 1, 2.

39 Kitchin, Big Data & Society 2014, S. 1, 10.

40 Margetts, The Promises and Threats of Big Data for Public Policy-Making.

41 ABIDA, Big Data – Lösung oder Problem, S. 13 f.

Literaturnachweise

ABIDA, Big Data – Lösung oder Problem? Dokumentation und Analyse der Bürgerkonferenzen, http://www.uni-muenster.de/Jura.itm/hoeren/itm/wp-content/uploads/ABIDA_B%C3%BCrgerkonferenzen_Ergebnisbericht.pdf (zuletzt abgerufen: 11/2018).

Anderson, The End of Theory: The Data Deluge Makes the Scientific Method Obsolete, https://www.wired.com/2008/06/pb-theory/ (zuletzt abgerufen: 11/2018).

Blum/Schubert, Prozesse – Der Policy-Cycle, in: Blum/Schubert (Hrsg.), Politikfeldanalyse, 104-144. Wiesbaden 2011.

Boyd, Privacy and Publicity in the Context of Big Data. Keynote WWW 2010, http://www.danah.org/papers/talks/2010/WWW2010.html (zuletzt abgerufen: 11/2018).

Boyd/Crawford, Critical Questions for Big Data. Information, Communication & Society 15(5), 662-679, DOI: 10.1080/1369118X.2012.678878.

Dell, The fast lane to building a smarter city. Case Study Fujian University. http://i.dell.com/sites/doccontent/corporate/case-studies/en/Documents/2015-fujian-university-10022453-big-data-center-cloud.pdf (zuletzt abgerufen: 11/2018).

Deloitte, Big data analytics for policy making. A study prepared for the European Commission (DG DIGIT), http://www.ngi-summit.org/wp-content/materials/EU_papers/DG_digit_study_big_data_analytics_for_policy_making.pdf (zuletzt abgerufen: 11/2018).

Dietrich, Was sind offene Daten? bpb-Dossier zum Thema „Open Data“ vom 26.10.2011, http://www.bpb.de/gesellschaft/medien/opendata/64055/was-sind-offene-daten?p=all (zuletzt abgerufen: 11/2018).

DIVSI, Studie zum Thema „Digitalisierte urbane Mobilität. Datengelenkter Verkehr zwischen Erwartung und Realität“, https://www.divsi.de/wp-content/uploads/2016/09/DIVSI-Studie-Digitalisierte-Urbane-Mobilitaet.pdf (zuletzt abgerufen: 11/2018).

Helbig et al., Will Democracy Survive Big Data and Artificial Intelligence?, Scientific American, vom 25. Februar 2017, https://www.scientificamerican.com/article/will-democracy-survive-big-data-and-artificial-intelligence/ (zuletzt abgerufen: 11/2018).

Henke et al., The age of analytics: Competing in a data-driven world. McKinsey Global Institute Report, http://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Analytics/Our%20Insights/The%20age%20of%20analytics%20Competing%20in%20a%20data%20driven%20world/MGI-The-Age-of-Analytics-Full-report.ashx (zuletzt abgerufen: 11/2018).

Hilbert, Big Data for Development: A Review of Promises and Challenges. Development Policy Review, 34(1): 135-174, DOI: 10.1111/dpr.12142.

Höchtl et al., Big data in the policy cycle: Policy decision making in the digital era, Journal of Organizational Computing and Electronic Commerce, 26(1-2), 147-169, DOI: 10.1080/10919392.2015.1125187.

Hoeren, Big Data und die Forderung nach Datenqualität, in: Hoeren/Kolany-Raiser (Hrsg.), Big Data zwischen Kausalität und Korrelation, S. 3-17, Münster 2016.

Jülicher, Von Big Data zu Big Impact? ADLAS Magazin für Außen- und Sicherheitspolitik 1/2016, S. 14-16.

Jülicher, Big Data in der Bildung – Learning Analytics, Educational Data Mining und Co., in: Hoeren/Kolany-Raiser (Hrsg.), Big Data zwischen Kausalität und Korrelation, S. 55-62, Münster 2016.

Kitchin, Big Data, new epistemologies and paradigm shifts, Big Data & Society 2014, 1-12, DOI: 10.1177/2053951714528481.

Malomo/Sena, Data Intelligence for Local Government? Assessing the Benefits and Barriers to Use of Big Data in the Public Sector, Policy & Internet 9(1), 7-27, DOI: 10.1002/poi3.141.

Margetts, The promises and threats of big data for public policy-making. The Policy and Internet Blog. http://blogs.oii.ox.ac.uk/policy/promises-threats-big-data-for-public-policy-making/ (zuletzt abgerufen: 11/2018).

Mureddu et al., A new roadmap for next generation policy making, in: Ferriero/Pardo/Qian (Hrsg.), Proceedings of the 6th international conference on theory and practice of electronic governance (ICEGOV2012), 62-66. Albany 2012.

Nash, Responsible research agendas for public policy in the era of big data. The Policy and Internet Blog, http://blogs.oii.ox.ac.uk/policy/responsible-research-agendas-for-public-policy-in-the-era-of-big-data/ (zuletzt abgerufen: 11/2018).

Poel et al., Data for Policy: A study of big data and other innovative data-driven approaches for evidence-informed policymaking, https://ofti.org/wp-content/uploads/2015/05/dataforpolicy.pdf (zuletzt abgerufen: 11/2018).

UN Global Pulse, Mining Indonesian Tweets to Understand Food Price Crises. Methods Paper, Februrary 2014, http://www.unglobalpulse.org/sites/default/files/Global-Pulse-Mining-Indonesian-Tweets-Food-Price-Crises%20copy.pdf (zuletzt abgerufen: 11/2018).

UN Global Pulse, The State of Mobile Data for Social Good Report. June 2017. http://unglobalpulse.org/sites/default/files/MobileDataforSocialGoodReport_29June.pdf (zuletzt abgerufen: 11/2018).

UN Global Pulse, Understanding Public Perceptions of Immunisation Using Social Media, http://www.unglobalpulse.org/sites/default/files/UNGP_ProjectSeries_Perception_Immunisation_2014_0.pdf (zuletzt abgerufen: 11/2018).

B. Meinungsvielfalt im Big-Data-Zeitalter – die verfehlte Frage nach der Filterblase (Matthias Möller und Steffen Uphues)

Stand: Februar 2018

Abstract: Meinungsvielfalt im Big-Data-Zeitalter

Die Informationen, die den Menschen zur Verfügung stehen, sind in solch einer Masse vorhanden, dass es dem Einzelnen **unmöglich** ist, **alle Inhalte** zu erfassen. Aufnahmefähiger ist an dieser Stelle die Technik. So werden mit Hilfe von Big-Data-Anwendungen die im Internet vorhandenen Informationen in einem ersten Schritt gesammelt. Im Anschluss können die Daten sortiert und analysiert werden, wodurch jedem Einzelnen **diejenigen Informationen** präsentiert werden können, die **aus seiner Sicht relevant** erscheinen. So geschieht es etwa bei der Facebook-Timeline, bei Suchmaschinenergebnissen, beim Online-Shopping oder bei Nachrichtenportalen. Zum einen bringt dieser Filter Vorteile mit sich, da eine manuelle Auswahl relevanter Inhalte mehr Zeit beanspruchen würde. Zum anderen sehen Kritiker in diesem Vorgehen jedoch die Gefahr einer **Filterblase**. Den Menschen würden nur noch Inhalte mit ihrer eigenen Meinung zugespielt, wodurch sich eine Spaltung der Gesellschaft – und sogar eine Gefährdung der Demokratie – ergeben könnte. An dieser Stelle gilt es, eine **differenzierte Betrachtung** anzustellen sowie Vor- und Nachteile zunächst einmal wertungsfrei herauszuarbeiten.

I. Das Phänomen der Filterblase

Die Filterblase ist eines dieser Schlagwörter, die momentan in aller Munde sind. Nicht zuletzt die Tatsache, dass der Begriff am 09.08.2017 neben vielen weiteren in den Duden aufgenommen wurde, unterstreicht den Eindruck, dass es sich hierbei um ein neuartiges Phänomen handelt. Das erste Mal tauchte der Begriff öffentlichkeitswirksam im 2011 erschienenen Buch „The Filter Bubble: What the Internet Is Hiding from You“ von

Eli Pariser auf. Pariser beschreibt den Zustand des Internets, welches von großen Unternehmen wie Google oder Facebook beherrscht werde. Anhand von Such- und Surfgewohnheiten sowie weiteren persönlichen Daten können Algorithmen personalisierte Suchergebnisse und Werbung etwa in Form einer individuellen Facebook-Timeline erstellen – unsere eigene Filterblase.

Die Meinungen von Experten und Journalisten verschiedener Fachrichtungen gehen bezüglich der Existenz einer solchen Filterblase stark auseinander. So vertreten neben Pariser weitere Stimmen die These der Filterblase,[1] welche auch Barack Obama in seiner Abschiedsrede am 10.01.2017 aufgriff.[2] Andere Stimmen stehen dem Vorliegen einer Filterblase kritisch gegenüber.[3]

Dem Begriff der Filterblase kann man sich aus verschiedenen Blickwinkeln nähern. Zunächst einmal gibt es die beiden zuvor angerissenen absoluten Ansichten: Zum einen könnte man die These aufstellen, dass sich jeder Mensch in einer Filterblase befindet. Diese Filterblase beinhaltet jegliche Informationen und Ansichten, die die Person zur Kenntnis genommen hat – einschließlich der individuellen Bewertung. Die andere Herangehensweise wäre, zu sagen, dass es eine Filterblase als solche nicht gibt. Der Begriff würde suggerieren, dass dem Einzelnen heteronom Inhalte zugespielt werden, wodurch sich die Ansichten und subjektiven Realitäten des Einzelnen bestimmen – ohne dass dieser die Möglichkeit hat, aus der „Blase“ zu entkommen.

Problematisch erscheint die Ansicht, gewisse Leute in eine Filterblase einordnen zu wollen und andere wiederum nicht.[4] Dies würde vorausset-

---

1 Jürgens/Magin/Stark; http://www.sueddeutsche.de/digital/nachrichten-in-der-filterblase-es-gibt-uebrigens-auch-noch-andere-meinungen-1.3433609 (zuletzt abgerufen: 11/2018).

2 https://qz.com/882755/in-his-farewell-address-obama-named-the-danger-in-our-social-media-filters-calling-it-the-great-sorting/ (zuletzt abgerufen: 11/2018).

3 Beispielhaft hierfür: http://www.zeit.de/2017/34/algorithmen-filterblase-meinungen-selbstbetrug (zuletzt abgerufen: 11/2018).

4 https://www.nzz.ch/feuilleton/filterblasen-und-aufgeblasene-thesen-wir-zwerge-unter-datenriesen-ld.144971 (zuletzt abgerufen: 11/2018).

zen, dass eine Grenzziehung möglich wäre, die sich mit der Frage auseinandersetzt: Ab wann bzw. unter welchen Bedingungen befindet sich ein Mensch in einer Filterblase? Es könnte ein Versuch unternommen werden, dies nach der Anzahl verschiedener Interessen zu bestimmen, die jemand verfolgt; oder nach der Anzahl konsumierter Meinungen bezüglich zur Kenntnis genommener Sachverhalte. Eine solche Einordnung erscheint jedoch weder umsetzbar noch zweckmäßig.

II. Weg von der Begrifflichkeit – hin zu den Fragestellungen

Ob eine Filterblase als solche existiert oder nicht, lenkt nach Meinung der Verfasser aber von den wirklich relevanten Fragestellungen ab.

Im Grunde geht es im Zusammenhang mit der Meinungsvielfalt darum, eine Grundlage zu schaffen, welche eine demokratische Meinungsfindung ermöglicht. Eine solche setzt voraus, dass eine gewisse Meinungsvielfalt dargeboten wird, die dem Einzelnen die Chance eröffnet, sich eine eigene Meinung zu bilden und diese als Ausdruck seines politischen Willens in den demokratischen Prozess einzubringen.

Mitte der 1930er Jahre nahm der erste deutsche Rundfunksender den Betrieb auf. Bis 1984 standen der Bevölkerung lediglich die öffentlich-rechtlichen Rundfunksender zur Verfügung – die dargebotene Meinungsvielfalt war somit begrenzt. In diesem Jahr stießen mit PKS (heute Sat. 1) und RTL plus (heute RTL Television) erste deutsche Privatsender hinzu – und dies war nur der Anfang. Heutzutage gibt es unzählige Fernsehsender sowie eine stetig wachsende Zahl an Onlineportalen, auf denen Neuigkeiten und Informationen veröffentlicht werden. Dies führt zum einen dazu, dass dem Einzelnen potentiell mehr Meinungen angeboten werden, mit denen er sich auseinandersetzen kann. Auf der anderen Seite besteht die Möglichkeit, sich gezielt Inhalte und Darstellungsweisen herauszusuchen, derer man sich bedienen möchte. Programme etwa, die auf eine bestimmte Bevölkerungsgruppe ausgerichtet sind, bieten dann womöglich eine tendenziöse und undifferenzierte Darstellung an; anders als früher die öffentlich-rechtlichen Sender, welche dem Anspruch als „Volksfernsehen“ gerecht werden und alle „bedienen“ mussten.

Mit dem wachsenden Einsatz von Big-Data-Anwendungen kommt hinzu, dass aufgrund einer Vielzahl von Daten – welche hauptsächlich aus dem Internet bzw. aus dem Internetverhalten des Einzelnen bezogen werden – Statistiken bezüglich der Interessen der Konsumenten mit deutlich höherer Aussagekraft aufgestellt werden können. Diese Big-Data-Anwendungen ermöglichen es, den Nutzern Inhalte zuzuspielen, welche für sie von besonderem Interesse sind. Aus dieser gesteigerten Diversität ergeben sich sowohl Chancen als auch Risiken, welche im Folgenden beleuchtet werden sollen.

III. Meinungsvielfalt im analogen Bereich

Diejenigen, die vom Vorliegen einer Filterblase ausgehen, sehen hierin häufig ein negatives Phänomen des digitalen Zeitalters; insbesondere, wenn in der Folge nicht nur ökonomische Entscheidungen beeinflusst, sondern auch gesellschaftspolitische Meinungsbilder manifestiert werden.

Zunächst ist jedoch festzuhalten, dass selbst im Zeitalter von Google und Facebook eine Meinungsbildung ebenso im analogen Leben stattfindet. Meinungen werden maßgeblich von der sozialen Realität, in der wir leben, beeinflusst – ob dies das Heimatdorf, die Familie, der Arbeitsplatz, der Fußballverein oder der Stammtisch ist.[5] Ebenso erfolgte die Auswahl der Nachrichteninformationen schon früher insofern „gefiltert“, als dass viele nur bestimmte Zeitungen und Zeitschriften (die ihnen gefielen) abonnierten und lasen. Wenngleich viele Redaktionen auf eine ausgewogene Berichterstattung achten, ist zumeist eine gewisse (gesellschafts-) politische Einfärbung sichtbar. Dies wird durch die momentane Situation des Journalismus verstärkt. Es vollzieht sich ein Prozess weg von der differenzierten Darstellung eines Sachverhalts und hin zu reißerischen Überschriften – das Überangebot und die daraus teils resultierende Quotenorientierung der Medien bringt es mit sich, dass mitunter der gewinnt, „der am lautesten schreit“.

---

5 http://digitalpresent.tagesspiegel.de/ich-lebe-in-keiner-filterbubble (zuletzt abgerufen: 11/2018).

IV. Big Data & Meinungsvielfalt

Fünf Jahre und vier Monate – so viel Lebenszeit verbringen Nutzer nach neuesten Studien durchschnittlich damit, sich in der Welt der sozialen Medien zu bewegen.[6] Sie klicken und wischen sich durch unzählige Nachrichten, Bilder und Videos, setzen Likes, kommentieren und diskutieren. Doch auch mehr als fünf Jahre reichen nicht annähernd aus, um sämtliche Online-Inhalte wahrzunehmen. Allein auf Instagram werden täglich 250 Millionen neue Stories gepostet.[7] Die vorhandenen Informationen müssen somit selektiert werden. Dies geschieht einerseits durch das Nutzerverhalten, indem Seiten besucht, geliked und abonniert werden. Neben den Nutzern sind es aber insbesondere auch Algorithmen, die bestimmen, was wir sehen und was nicht. Denn kein Klick bleibt unbemerkt; jede Handlung wird dem Algorithmus zugeführt, welcher für den Nutzer eine individuelle Timeline erstellt. Auch auf Plattformen wie Google sind sowohl der Mensch selbst als auch Algorithmen an der Ergebnisfindung beteiligt.

Das digitale (Suchmaschinen-)Zeitalter bietet so zwar die grundsätzliche Möglichkeit, aus dem „Meinungsspektrum des Stammtisches“ auszubrechen und sich aus einem breiteren Meinungspool zu informieren. Ohne Suchmaschinen wäre der Recherchierende meist auf die Quellen begrenzt, die ihm bekannt sind.[8] Da es aber soziale Realitäten sind, die maßgeblich das Verhalten im Internet beeinflussen und aufgrund derer das „individuelle Internetkonsumangebot“ von den Algorithmen errechnet wird, sehen viele die Informationsvielfalt durch die Suchmaschinen – ähnlich wie bei sozialen Netzwerken – wieder eingeschränkt.[9]

Insbesondere im Hinblick auf die Suchmaschinenanbieter wird dem entgegengehalten, dass der Einfluss auf die Meinungsbildung des Einzelnen womöglich überschätzt werde.[10] So sei insbesondere zu berücksichtigen,

---

6 https://t3n.de/news/viel-lebenszeit-verbringen-nutzer-809445/ (zuletzt abgerufen: 11/2018).

7 Laut Facebook-Status von Facebook-CEO Mark Zuckerberg, 26.07.2017.

8 Nolte, S. 552, 562.

9 Paal/Hennemann, S. 76.

10 Nolte, S. 552.

dass die digitale Meinungsbildung tatsächlich nur zu einem kleinen Teil mithilfe von Suchmaschinen erfolgen und die Informationsbeschaffung über mobile Apps eine viel größere Rolle einnehmen würde.[11] Auch hinsichtlich sozialer Netzwerke wird angeführt, dass häufig direkt Nachrichtenseiten angesteuert werden, während der Nachrichtenanteil auf Facebook im Vergleich zu beispielsweise Sport- oder den berühmt berüchtigten Katzenvideos gering sei.[12] Hinzu kommt, dass – im Jahr 2016 – laut einer Studie des Hans-Bredow-Instituts 72 Prozent der Befragten die Fernsehnachrichten als regelmäßig genutzte Nachrichtenquelle nannten; die sozialen Netzwerke nannten hier lediglich 31 Prozent[13] – ein weiterer Grund, die Bedeutung des Internets im Hinblick auf die Meinungsbildung nicht undifferenziert zu überhöhen.[14]

Im Internet haben aber jedenfalls eine Reihe von Faktoren eine Bedeutung, die zu einem verstärkenden Effekt hinsichtlich der Meinungsbildung führen können. Der vergleichsweise leichte Zugang zur Informationsverbreitung führt dazu, dass auf digitalen Plattformen viele Informationen unter dem Anschein journalistischer Arbeit ungeprüft abgegeben und weitergeleitet werden, mithin viele sogenannte Fake News existieren.[15] Die Verbreitung von Fake News wird zudem – im Vergleich zur „Stammtisch-Filterblase“ – dadurch verstärkt, dass die sozialen Medien die Möglichkeit der faktisch anonymen Äußerung ermöglichen.[16]

Weiterhin wird mithilfe von Social Bots versucht, die öffentliche Meinungsbildung im Netz zu beeinflussen. Social Bots sind Computerprogramme, die in sozialen Netzwerken eine menschliche Identität vortäuschen und wie diese agieren, d.h. Beiträge verfassen, liken, mit anderen kommunizieren. Tatsächlich stecken hinter Bots aber häufig Algorithmen von Meinungsmachern, die versuchen, die öffentliche Meinung in ihrem

---

11 Nolte, S. 552, 562 f.

12 http://www.sueddeutsche.de/wissen/erkenntnistheorie-der-mythos-von-der-filterblase-1.3254772 (zuletzt abgerufen: 11/2018).

13 Mehrfachnennungen waren möglich.

14 Hasebrink/Hölig, S. 17.

15 Paal/Hennemann, S. 76, 77.

16 Nolte, S. 552, 553.

Sinne zu beeinflussen.[17] Dem positiven Effekt der größeren Meinungsvielfalt im digitalen Zeitalter steht somit unter anderem ein sich durch Social Bots verstärkender negativer Effekt gegenüber, dass den Menschen gleiche und damit die eigenen Ansichten bestätigende Meinungen angezeigt werden und somit eine „Echokammer" entsteht.[18] Zu beachten ist diesbezüglich jedoch, dass wissenschaftliche Erkenntnisse darüber, inwiefern Social Bots tatsächlich Meinungsbilder beeinflussen können, noch nicht gegeben sind[19] und die Wirkweise von Social Bots möglicherweise überschätzt wird.[20]

V. Ökonomische Implikationen

Aus einem ökonomischen Blickwinkel betrachtet, erscheint der Einsatz von Big-Data-Anwendungen zur Personalisierung von Inhalten sinnvoll. Um die finanziellen Interessen zu verfolgen, geht es für Betreiber von Onlinemedien oder sozialen Netzwerken zunächst darum, die Nutzer auf der Webseite zu halten. Das alte Geschäftsmodell der Printmedien, sich über das Schalten von Werbeanzeigen zu refinanzieren, ist für Onlinemedien nur bedingt anwendbar.[21] An dieser Stelle ist es meist von Bedeutung, wie lange ein Nutzer auf einer Webseite verweilt und welche Artikel angeklickt werden. Dass einige Journalisten sich hierdurch zum Clickbaiting[22] verleiten lassen und der journalistische Anspruch auf der Strecke bleibt, ist ein weiteres Problem, auf welches an dieser Stelle jedoch nicht weiter eingegangen werden soll.

Ökonomische Interessen müssen ebenfalls berücksichtigt werden, wenn es um die Beurteilung der Glaubwürdigkeit von bzw. um das Vertrauen in

---

17 Milker, S. 216.

18 Drexl, S. 529.

19 Kind et al., S. 6.

20 Hegelich, S. 4/5.

21 https://www.heise.de/tp/features/Medien-in-der-Filterblase-Das-ist-nicht-nur-eine-Gefahr-sondern-eine-Tatsache-3830955.html (zuletzt abgerufen: 11/2018).

22 Clickbaiting meint eine Überschrift, welche eine sogenannte Neugierlücke (engl. „curiosity gap") aufweist. Die Überschrift hat nicht den Anspruch, den Text bestmöglich zu beschreiben, sondern möchte in dem Leser vielmehr durch das Anbringen von einzelnen reißerischen Begriffen die Neugier wecken und ihn dazu bewegen, durch Klicken den Volltext aufzurufen.

Suchmaschinenanbieter geht. Diese hätten schon allein aus wirtschaftlichen Gründen kein Interesse daran, Suchmaschinenergebnisse zu manipulieren, da – vorausgesetzt Manipulationen werden offenbart – die Nutzer das Vertrauen in den Anbieter verlieren würden und – da es bei Suchmaschinen keine Lock-in-Effekte durch Wechselkosten gibt – die Nutzer an andere Anbieter verloren gingen.[23]

VI. Meinungsvielfalt & der Mensch

In der Debatte rund um den Begriff der Filterblase wird meist ein Szenario dargestellt, welches hinsichtlich der Folgen für den Einzelnen teils etwas Bedrohliches, jedenfalls jedoch etwas Negatives beinhaltet. Eli Pariser hat etwa die Vermutung aufgeworfen, dass die Menschen intellektuell weniger gefordert würden.[24] Die ökonomischen Interessen stünden im Vordergrund und es ginge für Betreiber von Onlinemedien oder sozialen Netzwerken zunächst darum, die Nutzer auf der Webseite zu halten – hierfür ist ein Katzenvideo mitunter zielführender als ein anspruchsvoller Text.

Das Internet wartet neben einem riesigen Angebot an Wissen auch mit der Schilderung von Eindrücken und Gefühlen auf. Ausführungen zu zwischenmenschlichen Interaktionen, Reisen, Lebensbetrachtungen oder Ähnlichem anzuschauen und durchzulesen, bietet die Möglichkeit, seinen Horizont zu erweitern. Der menschliche Reflex, auf Unbekanntes zunächst mit Angst und Abwehrhaltung zu reagieren, könnte peu à peu abtrainiert werden, indem man sich mit fremden Kulturen, fremden Religionen – oder auf einer anderen Stufe gedacht – mit fremden Gefühlen beschäftigt. Die Meinungsvielfalt im Internet schafft somit zumindest abstrakt die Chance, das Verständnis für das Miteinander in der Bevölkerung zu fördern und die Entdeckung neuer Leidenschaften zu ermöglichen. Schon Adolph Knigge schrieb im Jahr 1788 in seinem Buch „Über den Umgang mit Menschen“: „Man glaubt es gar nicht, welch ein eintöniges Wesen man wird, wenn man sich immer in dem Zirkel seiner eigenen Lieblingsbegriffe herumdreht, und wie man dann alles wegwirft, was nicht

---

23 Nolte, S. 552, 563.

24 Pariser, The filter bubble – What the Internet is hiding from you.

unser Siegel an der Stirne trägt“.[25] Um den Menschen im Sinne von Knigge im Internet auf Entdeckungsreise ziehen zu lassen, muss die Medienkompetenz des Einzelnen gefördert werden. Das individualisierte Bereitstellen von Inhalten bietet viele Vorteile – auch auf soziologischer Ebene – und sollte nicht mit dem Kampfbegriff der Filterblase in eine unsachliche Auseinandersetzung verstrickt werden. Letztendlich trifft der Nutzer die Entscheidung, welche Webseite er besucht – so wie er die Entscheidung trifft, welches Buch er sich in der Bibliothek aus dem Regal zieht. Der Unterschied besteht darin, dass die Inhalte im Internet zahlreicher und teilweise ungeordnet sind; mit dieser Besonderheit muss sich der Mensch vertraut machen und dann für sich selber einen Weg finden, in seinem Interesse damit umzugehen.

Es kann durchaus sinnvoll sein, Inhalte zu filtern und sich mit einigen Dingen nicht auseinander zu setzen. Zart besaitete Menschen, welche sich niemals einen Horrorfilm ausleihen würden, sind sicherlich froh ob der Möglichkeit, durch Funktionen wie Ausblenden oder Blocken gewaltsame Inhalte in sozialen Netzwerken nicht angezeigt zu bekommen.[26] Daneben ist ein Filter auch im Hinblick auf die Informationsaufnahme des Einzelnen durchaus hilfreich. Den Menschen stehen immer mehr Informationen zur Verfügung. An dieser Stelle ist es nicht Fluch, sondern Segen, sich eines Filters zu bedienen, um die Inhalte und Informationen zu erhalten, welche für den jeweiligen Nutzer von Relevanz sind.

Ferner werden in der heutigen Gesellschaft Inhalte oftmals in einer hohen Geschwindigkeit, jedoch mit einer ebenso hohen Halbwertszeit in den Medien dargestellt. Dies führt unter anderem zu der Wahrnehmung, es passiere heutzutage mehr auf der Welt. Jede Woche ist eine neue Rede politischer Art zu hören, welche problematisiert, in was für einer „unruhigen Zeit“ wir uns doch befinden würden. Auch wenn Unruhe auf Empfindungen beruht und ein Vorliegen somit im Grunde subjektiv zu beurteilen ist, mag diese Formulierung angesichts der jüngeren deutschen Geschichte aus Sicht älterer Menschen zynisch klingen. Das Gefühl der Unruhe rührt wohl

---

25 Knigge, S. 83.

26 http://www.spiegel.de/netzwelt/web/facebook-und-die-filterblase-kolumne-von-sascha-lobo-a-1145866.html (zuletzt abgerufen: 11/2018).

weniger daher, dass es tatsächlich eine Bedrohungslage für die deutsche Bevölkerung gibt, sondern ist vielmehr von Medienhand geschaffen und hängt mit der Darstellung sowie der – sehr emotionalen und sprachlich absolut fehlerhaft mit immer wiederkehrenden Superlativen versehenen – Bewertung von Ereignissen zusammen. Die Langzeitfolgen von z. B. Eil- und Pushmeldungen für die psychische Konstitution des Einzelnen sind aufgrund der kurzen Zeit noch nicht erforscht. Dennoch wagen sich die Autoren so weit hervor, von negativen Auswirkungen auf Gelassenheit sowie Reaktion in Krisensituationen zu sprechen. In Anbetracht dessen erscheint es vorausschauend, sich der Echtzeit-Berichterstattung ein Stück weit zu entziehen.[27]

VII. Die Panik vor dem Sturz der Demokratie

Eine Aussage, die in letzter Zeit häufiger zu lesen war, lautete, die Demokratie sei durch eine Filterblase gefährdet.[28] So stellt der Historiker Niall Ferguson die These auf, die hohe Zahl der Amerikaner, die Facebook als ihre relevante Bezugsquelle für Nachrichten angibt, zeige, dass Facebook die Demokratie zerstöre. Nun ist zunächst einmal festzuhalten, dass die weite Verbreitung demokratischer Grundzüge für sich – zumindest nach Ansicht der Verfasser – eine Errungenschaft der modernen Gesellschaft ist, die es immer wieder aufs Neue zu erhalten gilt. Eine Demokratie setzt grundsätzlich ein gewisses Quäntchen Akzeptanz oder wenigstens Toleranz voraus. Über diese Charaktermerkmale verfügt jedoch nicht jeder Mensch und es ist der menschlichen Art auch nicht gänzlich fremd, dass das Verhalten von einer gewissen Eigennützigkeit geleitet wird. In der Folge wird es wohl auch in der Zukunft fortlaufend Menschen geben, deren Interesse darin liegt, ein Über- und Untergeordnetenverhältnis zu schaffen und gewisse andere Bevölkerungsgruppen von der Teilhabe an der Gesellschaft auszuschließen – sie unternehmen Angriffe auf die Demokratie. Im Grunde hat sich jedoch im Vergleich zu früher lediglich das Medium geändert, welches der Propaganda zur Wirkung verhelfen sollte.

---

27 https://www.basicthinking.de/blog/2016/10/18/filterblase/ (zuletzt abgerufen: 11/2018).

28 Schweiger, S. 135; http://www.zeit.de/2017/53/soziale-netzwerke-facebook-macht-niall-ferguson-historiker (zuletzt abgerufen: 11/2018).

War es früher noch das Radio oder später auch das Fernsehen, welches die Menschen mit tendenziösen Worten adressierte, so findet „Meinungsmache“ heute immer häufiger im Internet statt. Problematisch ist – und dies gilt es, differenziert zu diskutieren –, dass Inhalte und Meinungen den Einzelnen heutzutage deutlich schneller erreichen und dass der Umstand, dass viele Menschen öffentlichkeitswirksam auftreten können, dazu führt, dass bei dem Einzelnen womöglich die Wahrnehmung entsteht, diese Meinung wäre besonders stark. Hierdurch könnten sich die Fronten entscheidend verhärten. Sofern dies dazu führt, dass ein Diskurs über bedeutende gesellschaftspolitische Themen nicht mehr stattfindet, so ist zumindest ein Teilelement der Demokratie – der Meinungs*austausch* – bedroht. An dieser Stelle ist jedoch weniger die Politik gefordert, zu regulieren oder Verbote aufzustellen; vielmehr geht es darum, jeden Einzelnen anzutreiben, ein Bewusstsein in Bezug auf seinen Medienkonsum zu entwickeln. Demokratiegefährdendes Gedankengut entsteht im Kopf – und nicht im Internet. Was banal klingt, scheint im aktuellen Diskurs nicht jeder bei der Bewertung zu berücksichtigen. Solange es um strafbare Inhalte geht, sind die gesetzlichen Regelungen anzuwenden, welche eine Löschung und Sanktion anordnen. Bei allen anderen Inhalten gilt es, andere Meinungen und Ansichten zu akzeptieren – unabhängig davon, ob der Nachbar etwas im Vorgarten erzählt oder auf Twitter postet. Das beste Mittel für eine gesunde Demokratie ist weder Restriktion noch Regulierung – es ist der Dialog.

Mit Blick darauf könnte man dem Bedrohungsszenario berechtigterweise mit der Ansicht entgegentreten, dass das Internet-Zeitalter zu einer „Demokratisierung von Kommunikationsprozessen“ führt.[29] Die unendliche Informationsdichte des Internets sowie der einfache und (fast) überall verfügbare Zugang zu diesem sorgen dafür, dass dem Bürger heute so viele Informationsmedien zur Verfügung stehen wie nie zuvor – und dies zumeist unentgeltlich.

---

[29] Nolte, S. 552, 553.

VIII. Die Journalisten und ihre ganz eigene „Blase“

Sofern Journalisten von Filterblasen schreiben, muss berücksichtigt werden, dass sich auch die Journalisten selbst schwer tun, die kursierenden Meinungen in ihrer ganzen Vielfalt wahrzunehmen und in ihre Bewertungen mit einfließen zu lassen. So wurden Donald Trump im Vorfeld der Präsidentschaftswahl von den Medien – bis auf einige Ausnahmen – fast durchweg keine Chancen eingeräumt, Hillary Clinton zu besiegen.[30] Ob hinsichtlich dieser Fehleinschätzung der Wunsch Vater des Gedankens war oder andere Gründe eine Rolle spielten, lässt sich nicht abschließend klären. Es verfestigt sich jedoch auch im deutschsprachigen Raum der Eindruck, dass es den Medien momentan nicht gelingt, journalistisch das Meinungsspektrum der gesamten Bevölkerung abzubilden. Zu oft werden Meinungen verbreitet, anstatt Informationen zu liefern, welche dem Leser eine eigene Meinungsbildung möglich machen; zu selten werden Randgruppen mit vermeintlichen Mindermeinungen, unter anderem politscher Art, gehört und ohne Wertung in den Medien dargestellt. Dies könnte auch daran liegen, dass sich Journalisten häufig unter Kollegen bewegen und sich vermehrt auf Artikel anderer beziehen, ohne durch eigenen Gedankenzufluss einen inhaltlichen Mehrwert zu schaffen.[31] Einen Versuch, dem eigenen journalistischen Filter zu entfliehen, unternahm die Redaktion von „ZEIT online“ mit dem Projekt „#D17“.[32] Anlässlich der Bundestagswahl 2017 sollte in dieser Serie ein Bild der deutschen Bevölkerung geschaffen werden, welches jegliche Bevölkerungsschichten „zu Wort kommen lässt“. Ein erster Ansatz, der darauf hoffen lässt, dass die Medienlandschaft der Selbstreflexion zugänglich ist und in Zukunft wieder verstärkt ihre Rolle als Garant der Meinungsvielfalt wahrnimmt.

---

30 https://fivethirtyeight.com/features/there-really-was-a-liberal-media-bubble/ (zuletzt abgerufen: 11/2018); https://www.politico.com/magazine/story/2017/04/25/media-bubble-real-journalism-jobs-east-coast-215048 (zuletzt abgerufen: 11/2018).

31 https://www.heise.de/tp/features/Medien-in-der-Filterblase-Das-ist-nicht-nur-eine-Gefahr-sondern-eine-Tatsache-3830955.html (zuletzt abgerufen: 11/2018).

32 http://www.zeit.de/thema/d17; weitergeführt unter: https://www.zeit.de/thema/d18 (zuletzt abgerufen: 11/2018).

IX. Rechtliche Fragestellungen

Nicht selten wird in staatswissenschaftlicher Literatur[33] und in der Rechtsprechung des Bundesverfassungsgerichts[34] von der „demokratiekonstituierenden Bedeutung“ der Meinungsfreiheit gemäß Art. 5 Abs. 1 S. 1 1. Var. GG gesprochen. Die freie Meinungsäußerung setzt die Möglichkeit der freien Meinungsbildung und diese wiederum eine möglichst große Meinungsvielfalt voraus. Ständige Individualisierung gefährdet genau jene Meinungsvielfalt, da sie die Möglichkeiten, bestimmte Meinungen überhaupt wahrzunehmen, beschränken kann. Sämtliche Handlungsoptionen in Bezug auf eine vermeintliche Filterblase müssen sich also an dem Ziel messen lassen, eine möglichst große Meinungsvielfalt herzustellen.[35]

1. Kartellrecht

Die Meinungsvielfalt ist insbesondere dort bedroht, wo ein einziges – möglicherweise marktmächtiges – Unternehmen über eine beträchtliche Anzahl von Daten verfügt und somit Informationen für den Nutzer passgenau filtern kann. Zu denken wäre somit daran, die Meinungsvielfalt mit den Mitteln des marktmachtbegrenzenden Rechtsgebiets, dem Kartellrecht, zu erhalten. Es ist jedoch der Regelungszweck des Kartellrechts zu berücksichtigen: Dieser hat im Grundsatz allein die Chancengleichheit der wirtschaftlichen Akteure vor Augen; das Kartellrecht ist nicht dazu gedacht, die publizistische Meinungsvielfalt zu sichern[36] und kann somit nicht allein das Entstehen von Filterblasen verhindern.[37]

Über das Missbrauchsverbot hinaus wird daher diskutiert, ob weitere wettbewerbsrechtliche Handlungsmöglichkeiten genutzt werden sollen, z. B. die Offenlegung des Google-Algorithmus, eine auf Zwang beru-

---

33 Michael/Morlok, § 9, Rn. 201.

34 U.a. BVerfG im „Lüth“-Urteil, 1 BvR 400/57, NJW 1958, S. 257, 258.

35 Paal/Hennemann, S. 76, 77.

36 Dörr/Natt, S. 829, 843.

37 Paal, Vielfaltsicherung im Suchmaschinensektor, S. 34, 36.

hende strukturelle Entflechtung oder die Errichtung einer staatlich geförderten Alternative zu Google.[38] Diese Vorschläge stehen neben der Tatsache, dass es sich um massive Eingriffe in die Freiheit der Online-Dienstleister handeln würde, aus mehreren rechtspolitischen Gründen in der Kritik. Die staatlich geförderte Alternative zu Google würde nicht nur an tatsächliche und finanzielle Kapazitätsgrenzen stoßen[39], sondern müsste sich ebenso damit auseinandersetzen, dass alle Suchergebnisse auf Algorithmen zu stützen sind und es objektiv neutrale Suchergebnisse nicht gibt; eine staatliche Einflussnahme auf Suchergebnisse ist aus demokratischer Sicht als bedenklich einzustufen.

2. AGB-Recht

Als diskussionswürdig erscheint die Frage, inwiefern bereits auf vertraglicher Ebene die Zulässigkeit der Schaffung von Filterblasen beschränkt werden kann. Die Vereinbarung zwischen Nutzer und Dienstleister, dass Online-Angebote personalisiert werden, kommt nicht individualvertraglich, sondern durch Allgemeine Geschäftsbedingungen, die dem jeweiligen Vertrag beigefügt sind, zustande. Gem. § 307 BGB ist es dabei dem Verwender von AGB – hier den Online-Dienstleistern – untersagt, die Nutzer unangemessen zu benachteiligen. In der Regel stellen personalisierte Angebote jedoch gerade einen Vorteil dar, da der Nutzer das bekommt, wonach er sucht. Sofern es jedoch um Individualisierungen in meinungsrelevanten Meinungsangeboten geht, ist mit Verweis auf die durch Art. 5 Abs. 1 S. 1 Var. 1 GG geschützte Meinungsfreiheit eine Benachteiligung argumentativ begründbar.[40] Dann müsste allerdings dargelegt werden, dass ein differenzierter Meinungsbildungsprozess nicht nur im Gemeinwohlinteresse liegt, sondern auch Fragen der persönlichen Meinungsbildungsfreiheit berührt. Insofern eine unangemessene Benachteiligung iSd § 307 BGB jedoch angenommen wird, könnte eine AGB-Konformität dadurch hergestellt werden, dass die Einwilligung in die

---

38 Paal, Internet-Suchmaschinen im Kartellrecht, S. 997, 998.

39 Paal/Hennemann, S. 76, 78.

40 Hennemann, S. 544, 549.

Personalisierung zeitlich beschränkt wird (ggf. mit der Möglichkeit der Löschung der die Personalisierung betreffenden Daten) und der Nutzer wiederkehrend über die mit der Personalisierung einhergehenden Gefahren (u.a. Filterblasenbildung) zu informieren ist.[41]

3. Datenschutzrecht

Ab dem 25.05.2018 gilt die europäische Datenschutz-Grundverordnung (DS-GVO) und sodann muss die Datenverarbeitung den dort normierten Rechtmäßigkeitsanforderungen entsprechen. Das bedeutet insbesondere die Einhaltung diverser Transparenz- und Informationspflichten.[42] Gerade im Hinblick auf die oben festgestellten Wertungen des AGB-Rechts könnte es sinnvoll sein, die DS-GVO dahingehend zu überarbeiten, bei Angeboten mit konkreter Meinungsbildungsrelevanz die Einwilligungs- und Verarbeitungsvorschriften zu verschärfen; beispielhaft genannt werden wiederholte Informationspflichten oder „cooling-off"-Perioden.[43]

4. Medienrecht

Weitere Regulierungsansätze könnten sich aus dem Medienrecht und insbesondere aus dem Rundfunkstaatsvertrag ergeben. Wenn mit der herrschenden Ansicht jedoch vertreten wird, dass Suchmaschinen und soziale Netzwerke nicht unter den Begriff der Plattformen (§ 2 II Nr. 13 RStV) und der Telemedien mit journalistisch-redaktionell gestalteten Angeboten (§ 54 II 1 RStV) subsumiert werden können, sind auch wesentliche inhaltliche Regelungen nicht auf diese anwendbar.[44] Insofern wird vorgeschlagen, eine vielfaltsichernde Generalklausel in den Rundfunkstaatsvertrag aufzunehmen, um Suchmaschinen und soziale Netzwerke auch regulieren zu können.[45]

---

41 Hennemann, S. 544, 550.

42 Hennemann, S. 544, 546.

43 Paal/Hennemann, S. 76, 78.

44 Paal/Hennemann, S. 76, 77.

45 Paal/Hennemann, S. 76, 78.

Noch weitergehende Vorschläge sehen vor, im Rundfunkstaatsvertrag einen eigenen Regelungsbereich für Suchmaschinen zu schaffen.[46] Einer solch weitreichenden und umfangreichen Regulierung wird jedoch die Frage nach dem medienrechtlichen Regulierungsziel entgegengehalten.[47] Zwar könne eine Suchmaschine – schon allein weil der Nutzer dies so wünscht – gar nicht anders, als Suchergebnisse nach individueller Relevanz zu gewichten. Würde der Staat versuchen, ein objektiv richtiges Suchergebnis festzulegen, so wäre es schon gar nicht möglich, festzustellen, was objektiv richtig ist (da es eben um die individuelle Relevanz geht). Sobald der Staat aber beginnt, darüber zu urteilen, was objektiv richtig ist, würde dies zu einer wesentlich größeren Gefahr für die Meinungsbildung führen.[48] Somit sprechen aus demokratietheoretischen und verfassungsrechtlichen Gesichtspunkten gewichtige Argumente gegen eine Inhaltsregulierung von Intermediären.[49]

5. Wahl- und Parteienrecht

Problematisch wird die individualisierte Bereitstellung von Inhalten aus demokratietheoretischer Sicht insbesondere da, wo die Gefahr besteht, dass die Nutzer Meinungen von anderen politischen Parteien nicht mehr wahrnehmen. Somit könnte daran zu denken sein, dieser Gefahr in Wahlkampfzeiten über das Wahl- und Parteienrecht zu begegnen. Eine Option wäre z. B. ein Verbot des Einsatzes von Social Bots in Wahlkämpfen.[50] Zumindest wäre an Anzeige- und Transparenzpflichten für individuell zugeschnittene Werbung zu denken, wie sie beispielsweise von der Partei BÜNDNIS 90/DIE GRÜNEN in Bezug auf die Bundestagswahl 2017 auf Facebook geschaltet wurde.[51]

---

46 Kreile, S. 268, 272.

47 So Nolte, 552 ff. in Bezug auf Suchmaschinen. Er verneint bezüglich einer stärkeren Regulierung bereits die Gefährdungslage, d.h. die Gefahr von Filterblasen bei der Suchmaschinennutzung.

48 Nolte, S. 552, 563 f.

49 Drexl, S. 529, 535.

50 Drexl, S. 529, 543.

51 http://www.sueddeutsche.de/digital/wahlkampf-in-sozialen-medien-koennen-parteien-mit-personalisierter-werbung-die-wahl-manipulieren-1.3581781 (zuletzt abgerufen: 11/2018).

X. Fazit

Das Angebot an Meinungsvielfalt und die Bedeutung für die Meinungsbildung im Big-Data-Zeitalter sind noch nicht vollständig erforscht. Wenngleich eine vermeintliche Filterblase auch im analogen Leben existieren könnte, ist anzunehmen, dass das digitale Zeitalter diesen Effekt – trotz der zunächst größeren Pluralität – zumindest nicht mindert.

Jede rechtliche Maßnahme im Bereich der Filterblasen bewegt sich im Spannungsfeld zwischen dem Ziel, eine zu starke Macht privater Unternehmen bezogen auf das Angebot an Inhalten zu verhindern und der Gefahr einer zu starken staatlichen Einflussnahme. Zudem macht es die Schnelllebigkeit der technischen Entwicklungen im Internet schwierig, rechtliche Rahmenbedingungen aufzustellen. Das Recht allein kann die Problematik somit nicht vollständig erfassen, wenngleich einige der oben aufgezeigten Ansätze doch fruchtbar gemacht werden können.

Anstatt sich der Beschuldigung auszusetzen, man würde die Nutzer einseitig bevormunden, scheint es über rechtliche Maßnahmen hinaus insbesondere sinnvoll, den Nutzern selbst eine Differenzierung der Meinungsbilder zuzumuten. Denn: „Die allererste Filterblase ist der menschliche Verstand“; die Tatsache, dass den Nutzern in sozialen Medien verschiedene Inhalte angezeigt werden, liegt daran, dass jeder Mensch ein Individuum darstellt und damit keinem anderen gleicht.[52] Wichtig ist jedoch, dass der Nutzer in der Lage ist, die ihm angezeigten Inhalte richtig einzuordnen. Dazu ist es erforderlich, ein öffentliches Problembewusstsein bezüglich der Begriffe Filterblase, Fake News, Echo Chambers & Co. zu schaffen und insbesondere Maßnahmen zur Stärkung der Medienkompetenz zu ergreifen.[53] Zu denken wäre beispielsweise an die Schaffung eines Schulfaches „Medienkompetenz“.[54] Zumindest erscheint es sinnvoll, Fragen der Medienkompetenz in den jeweiligen Fachunterricht zu integrieren.

---

52 http://www.sueddeutsche.de/wissen/erkenntnistheorie-der-mythos-von-der-filterblase-1.3254772 (zuletzt abgerufen: 11/2018).

53 Grandjean, S. 565; Drexl, S. 529, 542.

54 https://www.heise.de/newsticker/meldung/Datenschutzbeauftragte-fordert-neues-Schulfach-Medienkompetenz-3658398.html (zuletzt abgerufen: 11/2018).

Daneben muss die Diskussion rund um Algorithmic Accountability fortgeführt werden. Eine – die technischen Besonderheiten berücksichtigende – Pflicht zur Offenlegung von Algorithmen bzw. zumindest die Verpflichtung zur Information der Nutzer über deren Funktionsweise ist ein wichtiges und sinnvolles rechtliches Instrument. In Verbindung mit der medienpädagogischen Fortbildung würde es dem Nutzer dadurch ermöglicht, selbstkritisch die ihm angezeigten Suchergebnisse und Timeline-Posts zu hinterfragen oder sogar Einfluss zu nehmen, zum Beispiel indem er bestimmte Seiten und Beiträge liked und abonniert, um so den Algorithmus zu beeinflussen.[55]

Literaturnachweise

Dörr/Natt, Suchmaschinen und Meinungsvielfalt, Ein Beitrag zum Einfluss von Suchmaschinen auf die demokratische Willensbildung**.** ZUM 2014, S. 829-846.

Drexl, Bedrohung der Meinungsvielfalt durch Algorithmen – Wie weit reichen die Mittel der Medienregulierung? ZUM 2017, S. 529-543.

Grandjean, Der Code als Gatekeeper: Vielfaltsicherung in Zeiten von Such- und Entscheidungsalgorithmen, Personalisierung und Fake-News. ZUM 2017, S. 565-572.

Hasebrink/Hölig, Reuters Institute Digital News Survey 2016 – Ergebnisse für Deutschland, https://hans-bredow-institut.de/uploads/media/Publikationen/cms/media/3ea6d4fed04865d10ad27b3f98c326d3a0ae6c29.pdf.

Hegelich, Invasion der Meinungsroboter. Analysen und Argumente, Konrad Adenauer Stiftung, September 2016, Ausgabe 221, http://www.kas.de/wf/doc/kas_46486-544-1-30.pdf?161222122757.

Hennemann, Personalisierte Medienangebote im Datenschutz- und Vertragsrecht. ZUM 2017, S. 544-551.

---

55 http://www.sueddeutsche.de/digital/facebook-filterblase-selbst-schuld-1.3479639 (zuletzt abgerufen: 11/2018).

Hilgefort, Datenschutzbeauftragte fordert neues Schulfach: Medienkompetenz, https://www.heise.de/newsticker/meldung/Datenschutzbeauftragte-fordert-neues-Schulfach-Medienkompetenz-3658398.html.

Jürgens/Magin/Stark, Ganz meine Meinung? Informationsintermediäre und Meinungsbildung – Eine Mehrmethodenstudie am Beispiel von Facebook, https://www.medienanstalt-nrw.de/service/pressemitteilungen/pressemitteilungen-2017/2017/august/expertise-zur-politischen-meinungsbildung-und-der-bedeutung-von-facebook-keine-voraussetzungen-fuer-filterblasen.html.

Kind et al., Social Bots – Thesenpapier zum öffentlichen Fachgespräch „Social Bots – Diskussion und Validierung von Zwischenergebnissen" am 26. Januar 2017 im Deutschen Bundestag, https://www.tab-beim-bundestag.de/de/aktuelles/20161219/Social%20Bots_Thesenpapier.pdf.

Knigge, Über den Umgang mit Menschen, 2. Auflage Hamburg 2016.

Kreile, Vorschläge zur Vielfaltsicherung bei Suchmaschinen im Rundfunkstaatsvertrag. ZUM 2017, S. 268-277.

Michael/Morlok, Grundrechte, 5. Auflage Baden-Baden 2015.

Milker, »Social-Bots« im Meinungskampf. ZUM 2017, S. 216-221.

Nolte, Hate-Speech, Fake-News, das »Netzwerkdurchsetzungsgesetz« und Vielfaltsicherung durch Suchmaschinen. ZUM 2017, S. 552-564.

Paal, Internet-Suchmaschinen im Kartellrecht. GRUR Int. 2015, S. 997-1005.

Paal, Vielfaltsicherung im Suchmaschinensektor. ZRP 2015, S. 34-37.

Paal/Hennemann, Meinungsvielfalt im Internet – Regulierungsoptionen in Ansehung von Algorithmen, Fake News und Social Bots. ZRP 2017, S. 76-78.

Pariser, The filter bubble – What the Internet is hiding from you, London 2011.

Schweiger, Der (des)informierte Bürger im Netz, Berlin 2017.

C. Big Data in Social Media & Wahlkampf (Barbara Kolany-Raiser, Nils Wehkamp und Lucas Werner)

Stand: März 2018

Abstract: Big Data in Social Media & Wahlkampf

Der Einsatz von Social Media im Wahlkampf hat bei allen größeren Parteien Einzug erhalten, besonders relevant sind hier Twitter, Facebook und Instagram. Durch die zunehmende gesellschaftliche Vernetzung und Nutzbarmachung von Big Data ergeben sich weitere neue Möglichkeiten zur Einflussnahme auf die politische Willensbildung, beispielsweise der Einsatz von Microtargeting oder Bots. Bei der Nutzung von Bots als Wahlkampfinstrument sowohl seitens der Parteien als auch privater Dritter, ergibt sich eine Kennzeichnungspflicht aus § 55 Abs. 1 RStV.

I. Einleitung

In diesem Dossier sollen die unterschiedlichen Methoden, wie Big Data und digitale Medien zum Wahlkampf genutzt werden können, erläutert werden. Es sollen die Vorteile sowie die potentiellen Gefahren beleuchtet werden, die mit ihrem Einsatz im politischen Wahlkampf einhergehen. Über allem schwebt immer die Frage, wo legitimer Wahlkampf aufhört und wo Manipulation anfängt. Sind speziell auf den Nutzer zugeschnittene Werbeanzeigen schon politische Manipulation oder noch legitimes Mittel der Werbung[1]? Sind Chatbots schon unethische Täuschung des Wählers oder lediglich eine zeitgemäße Methode, das Wahlprogramm interaktiv zu vermitteln?

---

1 http://www.sueddeutsche.de/digital/bundestagswahl-der-geheime-facebook-wahlkampf-der-parteien-1.3634351 (zuletzt abgerufen: 11/2018).

II. Wahlkampf in den sozialen Medien

Die Anzahl der Nutzer von sozialen Netzwerken ist im Jahr 2016 weltweit von knapp 1 Milliarde auf knapp 2,3 Milliarden gestiegen.[2] Darüber hinaus sind soziale Medien[3] die mit am schnellsten wachsenden Werbemärkte.[4] Längst sind diese Medien nicht mehr nur Plattformen für einen sozialen Austausch, sondern auch ein mächtiges Werkzeug für die Öffentlichkeitsarbeit von Firmen, aber auch Politikern und politischen Institutionen. Die Mehrzahl an deutschen Politikern und Parteien haben ein Facebookprofil und nicht nur Donald Trump nutzt Twitter, um zeitnah kurze Statements zum politischen Tagesgeschehen abzugeben. Dies hat für beide Seiten viele Vorteile. Da früher Pressemitteilungen durch Zeitungen und Journalisten aufgearbeitet werden mussten, gab es immer eine Instanz zwischen Wähler und Politiker. Durch die sozialen Medien fällt diese weg und dem Politiker ist es möglich, direkter mit seinen Wählern in Kontakt zu treten und vor allem zeitnah auf Ereignisse zu reagieren. Nutzer von sozialen Netzwerken verbreiten durch das Teilen von Beiträgen Nachrichten über den politischen Betrieb und diskutieren dabei auch untereinander.

Insgesamt hat diese neue Art des Wahlkampfes den Klassischen nicht komplett verdrängt, der Wahlkampf in sozialen Netzwerken ist neben den klassischen Kanälen nunmehr ein zusätzlicher Teil des politischen Marketingmixes.[5] Durch soziale Medien, als neuen Kommunikationskanal, eröffnen sich jedoch auch neue Möglichkeiten der politischen Kommunikation und Störung dieser, welche im Folgenden erläutert werden sollen.

---

2 Die Anzahl der Nutzer von sozialen Netzwerken ist im Jahr 2016 weltweit von knapp einer Milliarde auf knapp 2,3 Milliarden gestiegen.

3 Auch wenn die Definition für soziale Medien an sich breiter interpretiert werden kann, werden hier hauptsächlich die großen Netzwerke wie Twitter und Facebook betrachtet.

4 https://de.statista.com/outlook/220/137/social-media-werbung/deutschland

5 Vgl. auch Korte, Die Amerikanisierung der Wahlkämpfe, wonach sich das Internet „als zentrales Wahlkampfmedium entpuppt“.

1. Funktionsweise von sozialen Netzwerken

Um zu verstehen, was für eine Rolle soziale Medien in den politischen Diskussionen spielen, muss zunächst ihre Funktionsweise allgemein erläutert werden.

Innerhalb eines sozialen Netzwerkes bekommt jeder Teilnehmer mit seinem Profil die Möglichkeit, sich selbst nach außen darzustellen. Bei dem Teilnehmer kann es sich sowohl um eine Privatperson als auch um ein Unternehmen oder eine Institution handeln. Über sein Profil kann ein Nutzer je nach Netzwerk verschiedene Arten von Postings erstellen. Twitter beispielweise dient hauptsächlich dazu, kurze, 280 Zeichen lange Gedanken zu veröffentlichen. Dasselbe ist auch bei Facebook möglich, nur gibt es hier keine 280-Zeichen-Begrenzung. Des Weiteren besteht die Möglichkeit, Nachrichten oder Links von externen Seiten zu posten. Die Postings können von anderen Nutzern eingesehen werden,[6] welche den Post dann selbst teilen, liken oder kommentieren können.

Untereinander können sich Nutzer vernetzen, indem sie sich befreunden, Seiten liken oder jeweils Follower eines anderen Nutzers werden. Oft beinhaltet ein soziales Netzwerk auch einen Messenger Dienst, über den sich Nutzer private Nachrichten schicken können.

Beiträge in einem sozialen Netzwerk können jedoch neben dem privaten sozialen Austausch auch mit dem Ziel erstellt werden, Werbung[7] zu machen oder eine Meinung zu verbreiten.

Wie einflussreich eine Person oder ein Beitrag ist (bzw. wirkt) kann etwas vereinfacht an zwei Kennzahlen festgemacht werden. Zum einen an der Reichweite, d.h. wie viele Menschen einen Post zu Gesicht bekommen, zum anderen an der (wahrgenommenen) Relevanz. Zusammen bilden sie quasi das interne Belohnungssystem eines sozialen Netzwerkes. Der erste Punkt ist simpel; je mehr Menschen ein Posting erreicht, desto mehr

---

6 Die meisten Netzwerke bieten dem Nutzer jedoch auch die Möglichkeit, den Empfängerkreis einzuschränken.

7 Hier ist die Werbung durch Postings der Nutzer selbst gemeint. Zum zentralen Geschäftsmodell eines sozialen Netzwerkes gehört jedoch auch das Schalten eigener Werbung. Mit dieser Thematik beschäftigt sich das Dossier „Big Social Data“ (F.) intensiv.

Menschen können durch dieses beeinflusst werden. Die Reichweite hängt in sozialen Netzwerken vor allem von der Vernetzung des Autors und der Weiterverbreitung durch seine Follower oder Freunde ab (durch teilen oder retweeten). Die wahrgenommene Relevanz eines Beitrags, also wie allgemein bedeutend ein Nutzer einen Post wahrnimmt, ist dagegen komplexer. Ist ersichtlich, dass ein Posting oft geteilt wurde (bei Twitter beispielsweise wird die Anzahl der Retweets gezählt und angezeigt), erweckt dies den Eindruck, dass diese Meinung vielen Leuten als wichtig genug galt, um sie Ihren Freunden mitzuteilen. Gleiches gilt bei einer hohen Anzahl an Likes. Mit diesen können Nutzer ihre Zustimmung[8] in Bezug auf den geposteten Beitrag dem Autor und der Öffentlichkeit gegenüber ausdrücken. Wird ein Beitrag von einem Nutzer als relevant erachtet, steigt die Wahrscheinlichkeit, dass dieser sich intensiver mit dem Inhalt auseinandersetzt, wodurch auch die Chance erhöht wird, diesen Nutzer mit einer Meinung zu überzeugen.[9]

Die Funktionen der einzelnen sozialen Netzwerke unterscheiden sich im Detail von der oben beschriebenen Art und Weise. Zusammengefasst kann jedoch gesagt werden, dass die Grundfunktionen eines sozialen Netzwerkes im Posten, Teilen, Kommentieren und Liken von Beiträgen bestehen. Für die Relevanz oder wahrgenommene Relevanz sind die Anzahl der Likes, wie oft ein Beitrag geteilt wird, die Anzahl der Kommentare, sowie die Vernetzung des Autors wichtig.

2. Die Parteien in den sozialen Medien

Seitdem soziale Netzwerke nicht mehr nur für den privaten sozialen Austausch stehen, haben auch politische Akteure die sozialen Netzwerke als wirksame Werkzeuge der Öffentlichkeitsarbeit für sich entdeckt. Jede im Bundestag vertretene Partei besitzt ihre eigene Präsenz auf Facebook und Twitter, ebenso wie der Großteil der kleineren Parteien. Diese Plattform wird genutzt, um Werbung für die eigene Partei zu machen sowie Positionen zu vermitteln. Bei Twitter ist es in dieser Hinsicht ähnlich, auch

---

8 Bei Facebook können die Nutzer seit ein paar Monaten auch andere Emotionen wie Lachen, Staunen, aber auch Wut ausdrücken.

9 Vgl. Esch/Eichenauer.

hier haben sowohl Politiker als auch die Parteien ihre eigene Präsenz. Aufgrund der erzwungenen Kürze der Statements hat sich aber gerade Twitter für Politiker als attraktives Werkzeug erwiesen, um schnell kurze Kommentare zum aktuellen politischen Geschehen abzugeben. So können Meinungen und Ansichten von den Akteuren nahezu in Echtzeit verbreitet werden, ohne dass es einer Zusammenarbeit mit der Presse oder anderer Intermediärer bedarf.[10] Der Vorteil für beide Seiten liegt auf der Hand, da die eine Seite sich unverfälscht und schnell präsentieren und die Seite der Wähler einen ebenso schnellen und unverfälschten Eindruck gewinnen kann.[11] Bekanntester politischer Twitter-Akteur ist wohl Donald Trump, welcher mit seinen Tweets regelmäßig Debatten auslöst. Aber ebenso viele deutsche Politiker nutzen Twitter. Dies gilt sowohl für etablierte Politiker als auch für Aufsteiger.[12]

3. Politische Werbung von Nicht-Politikern

Neben den Berufspolitikern und Parteien, welche offiziell auf Facebook für ihre Sache werben, wird auch unter Privatpersonen politisch diskutiert. Während es früher durch räumliche Distanz schwieriger war, Gleichgesinnte zu finden, haben das Internet und vor allem die sozialen Medien dies für Menschen mit ähnlichen politischen Ansichten ebenfalls erleichtert. Die Grenze kann dabei auch fließend verlaufen. So können Facebook-Gruppen beispielsweise eine klare Präferenz zu einer Partei hin aufweisen und sogar von einem Parteimitglied geführt werden, während sie jedoch keinen offiziellen Kanal einer Partei darstellen.[13] In den Medien ist dann oft die Rede von „Partei X nahen Facebook-Gruppen“. Solche Gruppen können für eine Partei von Vor- oder Nachteil sein, denn diese hat zwar weniger Kontrolle über die geposteten Inhalte, muss sich für diese im Zweifelsfall jedoch nicht rechtfertigen.

Neben „normalen“ Wählern, welche im Netz eine politische Diskussion anstreben, kann es jedoch auch Gruppen oder Individuen geben, welche

---

10 Schlögl/Maireder; Bader et. al.

11 Bader et. al.

12 http://www.spiegel.de/politik/deutschland/bundestagsabgeordnete-auf-twitter-wer-wie-viel-schreibt-und-mit-wem-a-1041402.html (zuletzt abgerufen: 11/2018).

13 Vgl. Gertler.

ein Interesse daran haben, die Stimmung in den sozialen Netzen gezielt in eine Richtung zu manipulieren. Solche Gruppen können dann zahlreiche und aggressive Postings oder Kommentare zu einem bestimmten Thema absetzen. Zu beobachten war dieses Phänomen u.a. im US Präsidentschaftswahlkampf 2016. In Internetforen verabredeten sich dort Aktivisten der Alt-Right-Bewegung, um durch den Einsatz von Social Bots, Trollen oder der Verbreitung von Hate Speech den Wahlkampf zugunsten von Donald Trump zu beeinflussen.[14]

III. Neue Werkzeuge zur Störung des Wahlkampfes

Politik und gerade die Werbung für eigene politische Zwecke war in der Geschichte noch nie ein Feld, in dem Fairness, Ehrlichkeit und Transparenz als primäre Tugenden galten. Schon in einem Brief an seinen berühmten Bruder Markus Tulius riet Quintus Cicero seinem Bruder, möglichst vielen Menschen genau das zu versprechen, was sie hören möchten und den Kontrahenten mit so vielen Verleumdungen wie möglich zu überschütten.[15] Die Beeinflussung von Wählern zu den eigenen Gunsten gab es immer und wird es immer geben, und reicht von kleinen Marketingaktionen, um sich selbst im besten Licht dar stehen zu lassen, bis zu handfesten Manipulationsversuchen. Im Laufe der Jahre haben sich allerdings auch die Werkzeuge, welche der politischen Werbung zur Verfügung stehen, geändert. Während im alten Rom Verleumdungen durch Mund-zu-Mund-Propaganda weitergegebenen werden mussten, war das stalinistische Regime Mitte des 20. Jahrhunderts schon geübt darin, Fotos durch nachträgliches Retuschieren zu manipulieren und zu verbreiten.

Auch die politische Werbung in den sozialen Medien bleibt nicht von Manipulationsversuchen verschont, ist im Gegenteil sogar fast noch anfälliger. Dies hat mit mehreren Faktoren zu tun. Erstens ist der Umgang im Internet allgemein unpersönlicher und somit auch intransparenter. Durch

---

14 Laaf, Pöbeln mit Pepe the Frog, http://www.taz.de/!5351374; Lee, Understanding Trump's Troll Army, https://motherboard.vice.com/en_us/article/bmvnq4/understanding-trumps-troll-army; vgl. Kogel, Welche Rolle spielen rechte Trolle im Wahlkampf? Eine Analyse, https://motherboard.vice.com/de/article/599v88/welche-rolle-spielen-rechte-trolle-im-bundestagswahlkampf-eine-analyse.

15 Cicero.

technische Möglichkeiten ist außerdem die Verbreitung gerade auch mit begrenzten Ressourcen einfacher geworden.[16]

Im Folgenden sollen verschiedene Werkzeuge der Manipulation untersucht werden.

1. Manipulation durch Bots

Bots im Allgemeinen sind kleine Computerprogramme, welche automatisiert meist kleine, repetitive Aufgaben erledigen. Sie übernehmen dabei Arbeit, welche von einem Menschen als zu stumpfsinnig wahrgenommen werden würde und einfach in eine wiederholbare Struktur zu überführen ist. Die Bots gehen dabei vorher einprogrammierten Regeln nach. Obwohl Bots wie erwähnt meist für einfache repetitive Aufgaben genutzt werden, ist die Komplexität eines Bots theoretisch nach oben offen. Beispiel für komplexere Bots sind sog. Chatbots. Diesen ist anhand von Abgleichen mit Datenbanken möglich, komplexe Regelsysteme sowie menschliche Sprache zu verstehen und so auch einem Menschen gegenüber Antworten zu geben. Auf diese Weise ist es sogar möglich, einen menschlichen Gesprächspartner zu simulieren.[17]

Wie jegliche Technologie sind Bots an sich nicht per se gut oder schlecht. Tatsächlich sind Bots in vielen technischen Bereichen unverzichtbare Helfer, aber natürlich können sie auch zu schädigenden Zwecken eingesetzt werden. Entscheidend ist also die Absicht, mit der man sie einsetzt.

In sozialen Medien können Bots manipulativ eingesetzt werden, um in die oben beschriebenen Belohnungssysteme der Netzwerke einzugreifen. Social Bots sind Bots, welche in sozialen Netzwerken agieren und dabei versuchen, menschliches Verhalten zu imitieren. Das Ziel dabei ist meist, eine Meinung oder eine Ansicht innerhalb des sozialen Netzwerkes möglichst weit zu verbreiten oder eine bestimmte Meinung oder Person als wichtig, richtig oder relevant erscheinen zu lassen.[18] In der Praxis werden

---

16 Vgl. Neudert.

17 https://www.golem.de/news/ibm-watson-versteht-sprache-und-erstellt-dialoge-in-unity-games-1802-132897.html (zuletzt abgerufen: 11/2018).

18 Kind et al., S. 7.

etwa Facebook-Gruppen automatisch mit News gefüllt, bestimmte Beiträge, welche der eigenen Sache dienlich sind, automatisch möglichst weit verbreitet oder bei einem Post möglichst viele Likes generiert.[19]

Social Bots müssen nicht unbedingt manipulativ eingesetzt werden. So können Chatbots dazu verwendet werden, um den Wählern die Positionen einer Partei nahe zu bringen, beispielsweise eine digitale Tour durch das Wahlprogramm zu bieten. Einen Versuch unternahm die CSU im März 2017 mit einem in Facebook integrierten Chatroboter Paul. Dieser gab zu bestimmten Stichwörtern Antworten aus dem Wahlprogramm sowie einige augenzwinkernde Bemerkungen über politische Konkurrenten. Der Bot war dabei ausdrücklich als ein solcher gekennzeichnet.[20] Auch der Einsatz von Bots innerhalb der sozialen Netzwerke muss nicht unbedingt negativ sein. Die Inhalte sind durch das Parteiprogramm und das Wahlkampfteam im Vorhinein festgelegt. Die Platzierung einer Kampagne wird seit jeher von einem Wahlkampfteam übernommen. Auch ist es üblich, dass die Auftritte von Politikern und Parteien von einem Social-Media Team oder Mitarbeitern übernommen werden. Ob der Einsatz von Bots demnach ethisch legitim ist, ist keine Frage die Pauschal mit Ja oder Nein beantwortet werden kann. Die etablierten Parteien haben sich jedoch schon 2016 darauf geeinigt, auf Bots zur Verbreitung von Beiträgen und Meinungen zu verzichten, die AFD zog im April 2017 nach.[21]

Gerade in Bezug auf die AFD wird jedoch die Relevanz der nicht offiziellen Unterstützeraccounts deutlich. Auch wenn die Partei sich selbst offiziell von der Nutzung von Social Bots distanziert hat, vertraten viele der aktiven

---

19 http://www.zeit.de/digital/internet/2017-09/soziale-medien-bundestagswahl-manipulation-social-bots-trolle (zuletzt abgerufen: 11/2018).

20 Steppat, Die CSU hat einen neuen Chat-Roboter, http://www.faz.net/aktuell/politik/inland/wahlkampf-die-csu-hat-einen-neuen-chat-roboter-14996490.html (zuletzt abgerufen: 11/2018).

21 Wilkens, Justizminister Maas will, dass Parteien auf Social Bots verzichten, https://www.heise.de/newsticker/meldung/Justizminister-Maas-will-dass-Parteien-auf-Social-Bots-verzichten-3771556.html (zuletzt abgerufen: 11/2018); Merkel, Es gibt keine Social Bots der CDU Deutschlands, Statement auf Facebook, https://de-de.facebook.com/notes/angela-merkel/es-gibt-keine-social-bots-der-cdu-deutschlands/10154904442159820?comment_id=10154905582364820&reply_comment_id=10154939919293664&comment_tracking=%7B%22tn%22%3A%22R9%22%7D.

Social Bots AFD nahe Ansichten. So kaperten Aktivisten der Satirepartei Die PARTEI 30 Facebook-Gruppen, welche nach Angaben der PARTEI mithilfe von Bots aufgebaut und mit Inhalten gefüllt wurden, bevor die Leitung der Gruppe an echte AFD-Mitglieder abgegeben wurde.[22] Auch einer der größten AFD-Twitter-Accounts ist wahrscheinlich ein Bot.[23]

Umstritten ist jedoch der tatsächliche Einfluss von Bots. Die wissenschaftliche Forschung hierzu erweist sich als schwierig, da, um Erkenntnisse über Bots zu gewinnen, ebenjene erst einmal als solche identifiziert werden müssen. Von unterschiedlichen Studien werden hierzu verschiedene Definitionen genutzt, welche sich dem Phänomen lediglich von mehreren Seiten nähern. Eine oft verwendete Unterscheidung ist beispielsweise die Anzahl an Beiträgen. Ab einer bestimmten Anzahl an täglich abgesetzten Beiträgen, welche unüblich für menschliche Nutzer ist, würde dabei von einem Bot ausgegangen. Eine solche Definition weist offensichtliche Schwächen auf, da es auch bei menschlichen Nutzern teilweise recht üblich ist, mehr als 50 Tweets abzusetzen (so z. B. bei dem ehemaligen SPD- und Piraten-Politiker Christopher Lauer). Kategorien aufzustellen, um Bots von außen als Bots zu erkennen, ist vor allem aufgrund der inkrementellen Natur von Social Bots schwierig. Da Bots versuchen, menschliches Verhalten nachzuahmen, ist das Ziel, sie so zu programmieren, dass möglichst viele Parameter menschlichem Nutzerverhalten ähneln, wodurch die Unterscheidbarkeit erschwert wird.[24] Ebenfalls umstritten ist, inwiefern eine großflächige Beeinflussung durch Bots möglich ist.[25]

2. Trolle

Während Bots automatisch und weitestgehend autonom agieren, sind Trolle Menschen, welche durch gezielt provokante und/oder zahlreiche

---

22 Wirtgen, „Die Partei“ übernimmt 31 Facebook-Gruppen der AfD, https://www.heise.de/newsticker/meldung/Die-Partei-uebernimmt-31-Facebook-Gruppen-der-AfD-3820718.html (zuletzt abgerufen: 11/2018).

23 https://netzpolitik.org/2017/twitter-datenanalyse-bei-der-afd-die-falsche-balleryna/ (zuletzt abgerufen: 11/2018).

24 Ferrara et al.; hierzu auch ein anschaulicher Bericht vom 34C3 von Kreil, https://media.ccc.de/v/34c3-9268-social_bots_fake_news_und_filterblasen.

25 PwC, S. 17 ff.

Beiträge für eine Zuspitzung einer Diskussion sorgen.[26] Der Troll an sich hat seine Ursprünge bereits in den ersten Foren in den Vorläufern des Internets. Sie müssen dabei nicht unbedingt politisch sein. Unpolitische Trolle verfolgen einzig die Agenda der eigenen Belustigung. Ihnen geht es darum, durch Provokationen möglichst spektakuläre Reaktionen von ihren Opfern hervorzurufen.[27] Trolle mit einem politischen Hintergrund haben darüber hinaus auch ein politisches Ziel, dass sie durch ihr Getrolle direkt oder indirekt fördern wollen. Ein direkter Weg wäre dabei, Propagandamaterial zur Erreichung des politischen Ziels zu verbreiten.[28] Ein indirekter Weg wäre, eine sachliche Diskussion durch Provokation und Polemik dahingehend zu torpedieren, dass eine inhaltliche Auseinandersetzung nicht mehr möglich ist. Der Unterschied zu einem engagierten politischen Netznutzer liegt darin, dass ein Troll entweder mit Absicht Propaganda oder Falschmeldungen verbreiten will oder durch Provokationen das Klima einer Diskussion verderben möchte.[29]

Professionalisiert können solche Trolle eingesetzt werden, um eine Diskussionskultur gezielt zu manipulieren. Im Verdacht, sich solch professioneller Trolle zu bedienen, steht beispielsweise Russland, um prorussische und antiamerikanische Propaganda zu verbreiten.[30] Auch in Deutschland trieben zur Bundestagswahl 2017 organisierte Trolle ihr Unwesen. Ob diese staatlich gesteuert wurden, ist jedoch unklar.[31]

---

26 Indiana University, What is a troll?.

27 Buckels/Trapnell/Paulhus.

28 So mutmaßlich geschehen im US-Wahlkampf, vgl. Schuler, https://www.tagesschau.de/ausland/usa-russland-wahl-facebook-101.html.

29 Kampf, Wie rechte Internet-Trolle versuchten, die Bundestagswahl zu beeinflussen. Süddeutsche Zeitung, http://www.sueddeutsche.de/politik/manipulation-im-netz-wie-rechte-internet-trolle-versuchten-die-bundestagswahl-zu-beeinflussen-1.3875073 (zuletzt abgerufen: 11/2018).

30 https://www.welt.de/wirtschaft/webwelt/article139212744/Putin-leistet-sich-Troll fabrik-fuer-Netzpropaganda.html (zuletzt abgerufen: 11/2018).

31 https://faktenfinder.tagesschau.de/inland/manipulation-wahlkampf-101.html (zuletzt abgerufen: 11/2018); Brössler/Kahlweit, Putins Trolle und die Weltordnung, http://www.sueddeutsche.de/politik/fake-news-und-politik-putins-trolle-und-die-weltordnung-1.3748939 (zuletzt abgerufen: 11/2018).

3. Personalisierte Wahlwerbung

Eine weitere Möglichkeit zur Beeinflussung von Meinungsbildung und Wahlentscheidungen, verspricht man sich vom Einsatz personalisierter Wahlwerbung, dem sog. Microtargeting.[32]

Einer der größten Vorteile dessen liegt auf der Hand: Ein Wähler findet in beinahe jedem Wahlprogramm der verschiedenen Parteien einzelne Programmpunkte, die auf seine Zustimmung treffen. Ebenso wird er gewisse Ziele ablehnen; dass ein Wähler sich mit allen Forderungen aus einem Parteiprogramm identifizieren kann, stellt wahrscheinlich eher die Ausnahme dar. Aus dem Nutzerverhalten im Internet können nun die Präferenzen eines potentiellen Wählers ersehen werden. Ganz konkret könnte eine Partei diesem dann genau die Punkte eines Parteiprogramms präsentieren, die eher seine Zustimmung finden.

Bei Wahlwerbung an einen unbestimmten Adressatenkreis ist dies gerade nicht möglich. So wird die Effizienz der Wahlwerbung durch das Microtargeting auf ein neues Level gebracht. Diese Thematik soll hier jedoch nur der Vollständigkeit halber angesprochen werden. Einer ausführlichen Behandlung widmet sich das Dossier „Microtargeting – Gezielte Wähleransprache im Wahlkampf“ (E.).

4. Sonstige Beeinflussungen

In den letzten Jahren haben insbesondere auch sog. Leaks zunehmend an Bedeutung gewonnen. So wurden jüngst im vergangenen Wahlkampf um die US-Präsidentschaft Hackerangriffe durchgeführt, in denen vertrauliche Dokumente und E-Mails der Demokraten um Hillary Clinton erbeutet werden konnten. Diese wurden im Anschluss Stück für Stück veröffentlicht.

---

[32] Für die gezielte Wähleransprache werden auch Facekookdaten genutzt. Am 16.03.2018 wurde bekannt, dass das Unternehmen Camebridge Analytics, das im US-Wahlkampf für Donald Trump tätig war, sich in diesem Zusammenhang vermutlich illegalen Zugriff auf Facebookdaten von 50 Millionen Facebooknutzern verschafft hatte, https://www.heise.de/newsticker/meldung/Datenskandal-um-Cambridge-Analytica-Facebook-sieht-sich-als-Opfer-3999922.html (zuletzt abgerufen: 11/2018); genauere Angaben zur Involvierung von Cambridge Analytica in den US-Wahlkampf finden sich im Dossier „Microtargeting – Gezielte Wähleransprache im Wahlkampf“ (E.).

Zwar konnte trotz Spuren nach Russland nicht mit Sicherheit festgestellt werden, wer hinter diesen Angriffen steckte. Die Veröffentlichungen auf der Plattform WikiLeaks, in dessen Zuge beispielsweise der interne Machtkampf in den Reihen der Demokraten zwischen Hillary Clinton und Bernie Sanders publik wurde, dürfte für die demokratische Präsidentschaftskandidatin allerdings erhebliche Image-Schäden verursacht haben und löste auch Proteste unter den Anhängern von Bernie Sanders aus.[33]

Nachdem im Jahr 2015 bei einem Hackerangriff auf den deutschen Bundestag eine große Menge an Daten geklaut wurde, befürchteten Experten auch für den Bundestagswahlkampf 2017 ein ähnliches Szenario. Verfassungsschutzpräsident Maaßen und der damalige Innenminister de Maiziere hielten es für möglich, dass diese zur Diffamierung oder gezielten Desinformation vor der Wahl genutzt werden könnten.[34] Zwar gab es am Wahlwochenende dem Anschein nach vereinzelte Aktionen auf Twitter – diese standen mit den erbeuteten Daten allerdings nicht im Zusammenhang. Entgegen den Befürchtungen sind also entsprechende, groß angelegte Kampagnen ausgeblieben.

IV. Fake News

Die gezielte Verbreitung von Falschnachrichten ist ebenfalls ein Mittel, durch das in der Vergangenheit zumindest versucht wurde, auf Wahlentscheidungen Einfluss zu nehmen. Zwar ist das Verbreiten von Unwahrheiten zur Manipulation der politischen Meinungsbildung kein Problem, das erst in der digitalen Neuzeit seine Wurzeln findet. Jedoch wurde dieses Phänomen durch die neuen Möglichkeiten zur schnellen und weiten Verbreitung in sozialen Medien besonders relevant.[35]

---

33 https://www.washingtonpost.com/politics/hacked-wikileaks-emails-show-concerns-about-clinton-candidacy-email-server/2016/10/12/cdacbbd0-908f-11e6-a6a3-d50061aa9fae_story.html?utm_term=.1f5bad551ee5 (zuletzt abgerufen: 11/2018).

34 http://www.faz.net/aktuell/politik/bundestagswahl/bundestagswahl-angst-vor-cyberkriminalitaet-steigt-15121579-p2.html?printPagedArticle=true#pageIndex_2 (zuletzt abgerufen: 11/2018).

35 Siehe hierzu das Dossier „Fake News und Hate Speech“ (D.).

V. Rechtliche Einordnung

Gegen den Einsatz von sozialen Medien im Wahlkampf bzw. auch als generelles Kommunikationsmedium von Politikern sprechen für sich genommen in rechtlicher Hinsicht keine Bedenken. Selbiges gilt im Grundsatz auch für Versuche der Einflussnahme durch Private, deren Handlungsweisen meist auch in den Schutzbereich der Meinungsfreiheit fallen.

Andere Beurteilungen können sich allerdings dann ergeben, wenn die Beeinflussung in ihrer Art und Weise die üblichen Pfade verlässt oder gewisse inhaltliche Grenzen überschreitet.

So unterfällt der Einsatz von personalisierter Wahlwerbung, das sog. Microtargeting, den Beschränkungen des Datenschutzrechts. Fraglich ist weiterhin, wie der gezielte Einsatz von Falschmeldungen und Trollen rechtlich zu beurteilen ist. Im Mittelpunkt einer solchen Würdigung steht dabei insbesondere die Reichweite der Meinungsfreiheit aus Art. 5 Abs. 1 S. 1 Fall 1 GG sowie die Abwägung zwischen dieser mit den Rechten anderer, beispielsweise auch dem Allgemeinen Persönlichkeitsrecht aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG.

Bezüglich der ersten beiden Thematiken sei auf die gesonderte Behandlung in den Dossiers „Microtargeting – Gezielte Wähleransprache im Wahlkampf“ sowie „Fake News und Hate Speech“ verwiesen. Besonders brisant und daher auch Schwerpunkt der hier vorgenommenen rechtlichen Einordnung ist die Beeinflussung mittels Social Bots.

1. Einsatz von Social Bots

Der Einsatz von Bots ist an sich nicht verboten. In strafrechtlicher Hinsicht gelten für die von diesen generierten Inhalte wiederum die gleichen Maßstäbe wie für Aussagen von realen Personen im Netz, d.h. das Verbreiten von strafbaren Inhalten ist kein spezifisches Problem im Zusammenhang mit Social Bots. In zivilrechtlicher Hinsicht sei angemerkt, dass der Einsatz für sich bereits regelmäßig gegen die AGB des jeweiligen sozialen Netzwerks verstößt.[36] Die zivilrechtliche Durchsetzung stößt in der Praxis

---

[36] Milker, ZUM 2017, S. 216, 221.

freilich an ihre Grenzen, weil sie einen erheblichen Aufwand für ein Unternehmen bedeutet.[37]

Es wird vielmehr die Frage virulent, ob sich einerseits aus staatlichen Schutzpflichten die Notwendigkeit ergibt, die Beeinflussung der öffentlichen Meinungsbildung (gerade im Wahlkampf) in dieser Form zu verbieten. Zum anderen stellt sich die Frage, ob der Einsatz als Wahlkampfinstrument durch Parteien selbst verfassungsrechtlichen Bedenken begegnet.[38] Immerhin kommt diesen aufgrund ihrer grundrechtlich eingeräumten Sonderstellung aus Art. 21 GG eine besondere Verantwortung im Rahmen der politischen Willensbildung zu.[39] Schließlich stellt sich die Frage nach einer einfachgesetzlichen Kennzeichnungspflicht im Rahmen der Verwendung von Bots durch die Parteien im Wahlkampf.

2. Staatliche Schutzpflichten

In Betracht kommt hier insbesondere der Schutz der Meinungsfreiheit aus Art. 5 Abs. 1 S. 1 Fall 1 GG sowie der Freiheit der Wahl, Art. 38 Abs. 1 GG.

Die Meinungsfreiheit stellt in erster Linie ein subjektives Abwehrrecht dar, d.h. verpflichtet den Staat zur Unterlassung hoheitlicher Eingriffe in den Schutzbereich.[40] Unter Meinung werden Werturteile jeder Art verstanden, d.h. Äußerungen geprägt durch Elemente der Stellungnahme.[41] Daneben verpflichtet sie den Staat jedoch auch objektiv, die Voraussetzungen dafür zu schaffen und zu erhalten, dass der Bürger diese Freiheit auch real wahrnehmen kann.[42]

Ein Beispiel für die Beeinträchtigung dieser Wahrnehmungsmöglichkeit wäre, dass der öffentliche Kommunikationsbeitrag eines menschlichen

---

37 Beispielsweise sind einer Schätzung nach 9 bis 15 Prozent aller Twitter-User in den USA Bots, http://www.faz.net/aktuell/politik/bundestagswahl/bei-cyber angriffen-auf-bundestagswahl-feuern-auf-allen-kanaelen-15111925-p2.html. (zuletzt abgerufen: 11/2018).

38 Zumindest für den Bundestagswahlkampf 2017 haben alle Parteien den Verzicht des Einsatzes von Social Bots erklärt.

39 Vgl. hierzu auch Pötzsch, Die Deutsche Demokratie.

40 Dreier/Schulze-Fielitz, Art. 5, Rn. 121.

41 Maunz/Dürig/Grabenwarter, Art. 5 GG, Rn. 47.

42 Dreier/Schulze-Fielitz, Art. 5, Rn. 218.

Nutzers im Internet durch die Einkleidung in eine Flut von automatisiert erstellter Gegenrede durch einen Bot an Relevanz bzw. Wahrnehmbarkeit verliert. Weiterhin ist denkbar, dass die Diskussionskultur und -möglichkeit durch die Täuschung über die Menschlichkeit von Gesprächspartnern im Netz generell derart leidet, dass sich Nutzer vom Äußern einer Meinung im virtuellen Raum faktisch abhalten lassen.

Allerdings ist die Hürde sehr hoch, ab welchem Punkt den Staat eine Schutzpflicht trifft. Eine solche wird ausnahmsweise erst dann begründet, wenn ein Diskussionskanal komplett lahmgelegt wird,[43] m.a.W. die kommunikative Chancengleichheit nicht mehr gewährleistet werden kann. Solche schwerwiegenden Auswirkungen, die einen Handlungsbedarf des Gesetzgebers auslösen, sind bezüglich des Einsatzes von Bots bislang aber nicht ersichtlich.[44]

Vielmehr ist bei der rechtlichen Einordnung zu berücksichtigen, dass die Verbreitung von Meinungen oder „Stimmungsmache“ durch Bots selbst in den Schutzbereich der Meinungsfreiheit aus Art. 5 Abs. 1 S. 1 Fall 1 GG fällt. Ausgenommen von diesem Schutz sind allein reine Tatsachenbehauptungen, d.h. solche, die nicht meinungsbildend wirken, sowie unwahre Tatsachenbehauptungen.[45]

Dabei bleibt der Grundrechtsträger selbstverständlich der Programmierer des Bots. Dass die finale Fassung der getätigten Äußerung automatisiert erfolgt, ändert grundsätzlich nichts an dessen Schutzwertigkeit – der Grundrechtsschutz ist technikneutral.[46] Auf den ersten Blick scheint dieses Ergebnis gesellschaftlich nicht wünschenswert; jedoch würde andernfalls das Recht der Meinungsfreiheit von der Art und Weise der Kommunikation abhängen, was wiederum eine große Gefahr für die effektive Verwirklichung des Art. 5 Abs. 1 S. 1 Fall 1 GG darstellt.

---

43 Vgl. Milker, ZUM 2017, S. 216, 220.

44 Vgl. Dankert/Dreyer, K&R 2017, S. 73, 76.

45 Zum Teil unterschiedlich beurteilt wird, ob reine Schmähkritik und Formalbeleidigungen bereits aus dem Schutzbereich der Meinungsfreiheit ausgeschlossen sind oder – nach hier vertretener Ansicht – zwar dem Schutzbereich unterfallen, in der Abwägung jedoch hinter dem Allgemeinen Persönlichkeitsrecht zurückstehen müssen. Siehe hierzu Epping/Hillgruber/Schemmer, Art. 5, Rn. 4.

46 Steinbach, ZRP 2017, S. 101, 102.

Der Grundsatz der Freiheit der Wahl erfordert nicht nur, dass der Akt der Stimmabgabe frei von Zwang und unzulässigem Druck bleibt, sondern ebenso, dass die Wähler ihr Urteil in einem freien, offenen Prozess der Meinungsbildung gewinnen und fällen können.[47] Mithin ist auch die Phase des Wahlkampfes umfasst. Allerdings sind auch hier die Grenzen, ab wann eine derart intensive Beeinträchtigung der Freiheit der Wahl vorliegt, dass den Gesetzgeber eine Handlungspflicht trifft, hoch gesteckt. Im Ergebnis gewährleistet Art. 38 Abs. 1 GG daher auch keinen Schutz davor, von Privaten über die Relevanz von Äußerungen oder deren Wahrheitsgehalt getäuscht zu werden. Es besteht somit auch hier keine Schutzpflicht seitens des Staates.[48]

Vielmehr ist es notwendig, dass der Bürger eine Kompetenz dafür entwickelt, wie man welche Äußerungen im Netz einzuordnen hat. Es bedarf zudem eines Bewusstseins, dass eine gewisse Qualitätskontrolle, wie man sie bei seriösen Medien erwarten kann, bei zahlreichen Informationsquellen im Netz gerade nicht stattfindet. Schließlich sei auch darauf hingewiesen, dass es trotz sicherer Kenntnis vom Einsatz solcher Bots auch im Wahlkampf ohnehin empirisch ungewiss ist, welche Relevanz sie für die öffentliche Meinungsbildung und letztendlich für Wahlergebnisse besitzen.[49]

3. Einsatz durch die Parteien als Wahlkampfinstrument

Für staatliche Stellen gelten aufgrund deren Grundrechtsbindung aus Art. 1 Abs. 3 GG sowie des Rechtstaatsprinzips aus Art. 20 Abs. 3 GG bei an die Öffentlichkeit gerichteten Informationstätigkeiten besondere Anforderungen – deren Mitteilungen unterliegen dem Gebot der Sachlichkeit, Richtigkeit und Vollständigkeit und müssen insgesamt verhältnismäßig sein.[50] Hieraus ergibt sich, dass der Einsatz von Social Bots bei staatlicher Kommunikation in geeignetem Maße gekennzeichnet werden

---

47 Maunz/Dürig/Klein, Art. 38, Rn. 107.

48 Steinbach, ZRP 2017, S. 101, 105.

49 Jungherr, Das Internet in der politischen Diskussion: Forschungsstand und Perspektiven, S. 297.

50 M.w.N. Dankert/Dreyer, K&R 2017, S. 73, 76.

muss.[51] Im Hinblick auf das Gebot der staatsfreien Willensbildung bei Wahlen verbietet sich jedoch ohnehin eine Einflussnahme staatlicher Stellen im Wahlkampf – nichts anderes gilt auch für Versuche der staatlichen Beeinflussung aus dem Ausland (u.a. auch Geheimdienste), wobei sich letzteres auch aus dem völkerrechtlichen Einmischungsverbot ergibt.[52]

Trotz der bereits angesprochenen Sonderstellung der Parteien aus Art. 21 GG sind diese letztlich privatrechtliche Organisationen. Daraus folgt, dass sie gerade nicht den gleichen Anforderungen wie staatliche Stellen unterliegen. Zwar mag die Offenlegung der Nutzung von Social Bots aus Gründen der Transparenz wünschenswert sein – eine Pflicht hierzu ergibt sich bei der Kommunikation mittels Social Bots aus verfassungsrechtlichen Gesichtspunkten allerdings nicht.[53]

4. Kennzeichnungspflicht aus dem Rundfunk- und Staatsvertrag

Eine Kennzeichnungspflicht kann sich hingegen aus § 55 Abs. 1 RStV ergeben, der besagt:

„Anbieter von Telemedien, die nicht ausschließlich persönlichen oder familiären Zwecken dienen, haben folgende Informationen leicht erkennbar, unmittelbar erreichbar und ständig verfügbar zu halten:

1. Namen und Anschrift sowie
2. Bei juristischen Personen auch Namen und Anschrift des Vertretungsberechtigten.“

Voraussetzung dafür ist zunächst, dass es sich bei z. B. durch Social Bots erstellten Nutzerprofilen in sozialen Netzwerken um ein eigenständiges Telemedium handelt. Maßgeblich hängt dies von dem Grad der Eigenständigkeit und Ausgestaltungsmöglichkeit ab – dies hängt wiederum von den bereit gestellten Funktionen des jeweiligen Netzwerks ab.

Bei den hier vordergründig behandelten Netzwerken Facebook und Twitter bestehen gesteigerte Gestaltungsmöglichkeiten durch Bestimmung von

---

51 M.w.N. Dankert/Dreyer, K&R 2017, S. 73, 76.

52 M.w.N. Steinbach, ZRP 2017, S. 101, 104.

53 So i.E. auch Steinbach, ZRP 2017, S. 101, 105.

Profilbildern, Textbereichen u.a., sodass diese im Ergebnis eines Impressums bedürfen.[54]

Die Ausnahme vom Anwendungsbereich des § 55 Abs. 1 RStV (persönliche oder familiäre Zwecke) ist restriktiv zu verstehen.[55] Zwar bedeutet der Einsatz von Social Bots zur Kommunikation, auch politisch geprägter Inhalte, nicht automatisch, dass keine persönlichen oder familiären Zwecke verfolgt werden. Soweit es jedoch gezielt um den Einsatz zur Einflussnahme der öffentlichen Meinungsbildung geht (wie der Fall typischerweise beim Einsatz durch Parteien liegen dürfte), sind die von Bots gesteuerten Nutzerprofile jedoch kennzeichnungspflichtig.[56] Somit muss der Urheber des Social Bots seine Identität offen legen.

VI. Fazit

Ist es demnach angebracht, die Verwendung von Big-Data-gestützten Anwendungen zur Beeinflussung der politischen Meinungsbildung mit Sorge zu betrachten? Ein elementarer Bestandteil einer jeden Demokratie ist die freie Willensbildung des Wählers, die in Gefahr geraten könnte. Allerdings gehört zur freien Willensbildung auch die Freiheit des Wählers, seine Informationsquellen selbst auszuwählen und deren Glaubwürdigkeit selbst zu beurteilen. Dass dies im Zuge der fortgeschrittenen Digitalisierung, der damit eröffneten Unbegrenztheit an Informationsquellen und der Schnelllebigkeit des Internets ein sehr viel komplexerer Vorgang geworden sein dürfte, lässt sich nicht ernsthaft in Abrede stellen. Auch der Einsatz von neuen technischen „Errungenschaften“ verschärft dieses Unterfangen. So ist beispielsweise der tatsächliche Einsatz von Social Bots (auch) zur Meinungsmache mittlerweile unbestritten. Big Data kann selbst aber auch zur Entschärfung der Problematik beitragen. So werden beispielsweise Big-Data-basierte Anwendungen zur Enttarnung von Bots oder ganzen Bot-Netzwerken eingesetzt.[57]

---

54 Spindler/Schuster/Micklitz/Schirmbacher, § 5, Rn. 19.

55 Hahn/Vesting/Held, § 55 RStV, Fn. 27a.

56 Dankert/Dreyer, K&R 2017, S. 73, 77.

57 Kind et al.

Zur Entwarnung kann außerdem angeführt werden, dass über den tatsächlichen Einfluss auf die Willensbildung durch neuere Wahlkampfinstrumente bislang nur spekuliert werden kann. Zudem bedeuten die aufgezeigten Entwicklungen keineswegs nur Risiken. Die erweiterten Kommunikationsmöglichkeiten insbesondere zwischen Parteien und dem Bürger können dazu beitragen, einer sich in letzter Zeit abzeichnenden Politikverdrossenheit entgegenzuwirken. Besonders effektiv dürfte es sein, zukünftigen, potentiellen Wählern bereits in jungen Jahren eine gewisse Internet- bzw. Sozialmedienkompetenz an die Hand zu reichen, um sich über Beeinflussungen zumindest bewusst zu werden und seine Meinungsbildung aus dieser Erkenntnis heraus zu reflektieren.

Zusammenfassend lässt sich also wie so oft sagen, dass Politik und Gesellschaft es selbst in der Hand haben, die Auswirkungen der dargestellten Entwicklungen in eine positive Richtung zu lenken.

Literaturnachweise

Bader et al., Die Wahl in 140 Zeichen – Twitter als Kommunikationsplattform für Politik, Medien und Bürger im Bundestagswahlkampf 2013, Politische Psychologie 2015, S. 5-22.

Buckels/Trapnell/Paulhus, Trolls just want to have fun. Personality and Individual Differences, 67, 97-102. https://doi.org/10.1016/j.paid.2014.01.016 (zuletzt abgerufen: 11/2018).

Cicero, Wie man eine Wahl gewinnt: Der antike Ratgeber von Quintus Tullius Cicero, 1. Auflage Berlin 2013.

Dankert/Dreyer, Social Bots: Grenzenloser Einfluss auf den Meinungsbildungsprozess?, K&R 2017, S. 73-78.

Dreier, Grundgesetz Kommentar, 3. Auflage Tübingen 2013.

Epping/Hillgruber, Beck´scher Online-Kommentar Grundgesetz, 35. Edition München 2017.

Esch/Eichenauer, Verfahren zur Messung der Kommunikationswirkung im Internet und bei Social Media, in: Esch/Langner/Bruhn (Hrsg.), Handbuch Controlling der Kommunikation, Wiesbaden 2016.

Ferrara et al., The rise of social bots, Communications of the ACM 2016, 59(7), S. 96-104.

Gertler, Zwei Paradigmen nebeneinander: Meinungsbildung durch klassische vs. interaktive Medien, in: Friedrichsen/Kohn (Hrsg.), Digitale Politikvermittlung, Wiesbaden 2015.

Hahn/Vesting, Beck´scher Kommentar zum Rundfunkrecht, 3. Edition München 2012.

Indiana University, What is a troll? https://kb.iu.edu/d/afhc.

Jungherr, Das Internet in der politischen Kommunikation: Forschungsstand und Perspektiven, Politische Vierjahresschrift 2017, https://www.nomos-elibrary.de/10.5771/0032-3470-2017-2-284/das-internet-in-der-politischen-kommunikation-forschungsstand-und-perspektiven-jahrgang-58-2017-heft-2?page=1.

Kind et al., Social Bots – Thesenpapier zum öffentlichen Fachgespräch „Social Bots – Diskussion und Validierung von Zwischenergebnissen“ am 26. Januar 2017 im Deutschen Bundestag, https://www.tab-beim-bundestag.de/de/aktuelles/20161219/Social%20Bots_Thesenpapier.pdf.

Korte, Die Amerikanisierung der Wahlkämpfe, Bundeszentrale für politische Bildung 2017, http://www.bpb.de/politik/wahlen/249643/die-amerikanisierung-der-wahlkaempfe.

Maunz/Dürig, Grundgesetz-Kommentar, 79. Auflage München 2016.

Milker, “Social Bots” im Meinungskampf, Wie Maschinen die öffentliche Meinung beeinflussen und was wir dagegen unternehmen können, ZUM 2017, S. 216-222.

Neudert, Computational Propaganda in Germany: A Cautionary Tale, University of Oxford – Working Paper No. 2017.7, http://blogs.oii.ox.ac.uk/politicalbots/wp-content/uploads/sites/89/2017/06/Comprop-Germany.pdf.

Pötzsch, Die Deutsche Demokratie. 5. Auflage Bonn 2009, http://www.bpb.de/politik/grundfragen/deutsche-demokratie/39317/parteien?p=all.

PwC, Social Bots: Gefahr für die Demokratie?, Whitepaper mit Handlungsempfehlungen für Unternehmen, Medien und Politik, https://www.pwc.de/de/technologie-medien-und-telekommunikation/social-bots-gefahr-fuer-die-demokratie.pdf.

Schlögl/Maireder, Struktur politischer Öffentlichkeiten auf Twitter am Beispiel österreichischer Innenpolitik/Public spheres and twitter: The case of austrian domestic politics, Österreichische Zeitschrift für Politikwissenschaft 2015, S. 16-31, https://search.proquest.com/docview/1690371191?accountid=14597.

Spindler/Schuster, Recht der elektronischen Medien, 3. Auflage München 2015.

Statista GmbH, Social-Media-Werbung, https://de.statista.com/outlook/220/137/social-media-werbung/deutschland# (zuletzt abgerufen: 11/2018).

Steinbach, Social Bots im Wahlkampf, ZRP 2017, S. 101-104.

D. Fake News und Hate Speech (Barbara Kolany-Raiser und Lucas Werner)

Stand: Juni 2018

Abstract: Fake News und Hate Speech

Fake News und Hate Speech sind keine neuen soziologischen Phänomene, sondern gelangten in neuerer Zeit durch die einfache Verbreitungsmöglichkeit von Kundgaben im Internet zu vermehrtem Aufsehen. In rechtlicher Hinsicht haben die Begriffe keine eigenständige Bedeutung; die Einordnung als Fake News oder Hate Speech führt unter diesem Gesichtspunkt also zu keinem Mehrwert. Ob das Netzwerkdurchsetzungsgesetz (kurz NetzDG) Abhilfe schaffen kann und ob es vor allem verfassungs- und europarechtskonform ist, wird derzeit in vielerlei Hinsicht bezweifelt.

I. Einleitung

Unter dem Begriff Fake News versteht man laut Duden „in den Medien und im Internet, besonders in den Social Media, in manipulativer Absicht verbreitete Falschmeldungen“.[1] Die Motive dahinter sind verschiedener Natur – so können beispielsweise kommerzielle Interessen zur Verbreitung von Fake News verleiten: Ein Portalbetreiber möchte mit gefälschten Sensationsmeldungen möglichst viele Seitenaufrufe erzielen, um durch auf seiner Webseite geschaltete Werbung entsprechende Werbeeinnahmen zu generieren.[2] Andererseits werden Falschmeldungen aber auch gezielt zur Manipulierung der öffentlichen Meinungsbildung eingesetzt. Dies spiegelt sich auch in der Auffassung der von der EU-Kommission eingesetzten Expertengruppe wieder: „Disinformation as defined in this

---

1 http://www.duden.de/rechtschreibung/Fake_News/ (zuletzt abgerufen: 11/2018).

2 http://www.zeit.de/2016/52/fake-news-hersteller-unternehmen-mazedonien (zuletzt abgerufen: 11/2018).

Report includes all forms of false, inaccurate, or misleading information designed, presented and promoted to intentionally cause public harm or for profit."[3]

Hate Speech, oder auch das weniger etablierte deutsche Pendant „Hassrede", dient als Oberbegriff für beleidigende, diskriminierende oder volksverhetzende Ausdrucksformen insbesondere im Internet.[4] Das Verständnis, was genau dieser Kategorie unterfällt, ist dabei umstritten, hängt es doch insbesondere vom jeweiligen Kontext ab.[5] Auch kann es sowohl ganze Gruppen als auch Individuen herabwürdigen – die Grenzen zur „gewöhnlichen", persönlichen Beleidigung sind daher fließend.

Beiden Erscheinungen sind gemein, dass sie in jüngster Zeit große Aufmerksamkeit erlangt haben. Dabei ist weder die Verbreitung von Unwahrheiten noch die Diffamierung einzelner Personen sowie ganzer Minderheiten eine neuartige Erscheinung, die mit dem Internet oder der Etablierung von Social Media entstanden ist.[6] Allerdings tragen zwei wesentliche Gesichtspunkte dazu bei, dass diese durch die fortschreitende Digitalisierung eine neue Bedeutung erhalten haben, die mittlerweile als gesellschaftliches Problem angesehen wird. Zum einen gewährleistet das Internet weitgehende Anonymität bei der Äußerung strafbarer Inhalte und lässt angesichts der geringen Gefahr von strafrechtlicher Verfolgung die Hemmschwelle sinken. Angemerkt sei an dieser Stelle jedoch, dass die anonyme Kommunikation im Netz an sich nicht verwerflich ist – sie kann

---

3 Europäische Kommission, S. 35.

4 Bereits 1997 erließ der Europarat eine Empfehlung zum Umgang mit Hassreden. Die dort verwandte Definition umfasst „ […] jegliche Ausdrucksformen, welche Rassenhass, Fremdenfeindlichkeit, Antisemitismus oder andere Formen von Hass, die auf Intoleranz gründen, propagieren, dazu anstiften, sie fördern oder rechtfertigen, einschließlich der Intoleranz, die sich in Form eines aggressiven Nationalismus und Ethnozentrismus, einer Diskriminierung und Feindseligkeit gegenüber Minderheiten, Einwanderern und der Einwanderung entstammenden Personen ausdrücken" und dient heute oftmals als Ausgangspunkt für die Erfassung des Begriffs Hate Speech, http://www.egmr.org/minkom/ch/rec1997-20.pdf (zuletzt abgerufen: 11/2018).

5 Vgl. Stefanowitsch, S. 12.

6 Vgl. auch Guggenberger, ZRP 2017, S. 98.

sogar in positiver Hinsicht zum Meinungsaustausch animieren.[7] Zum anderen entfalten entsprechende Äußerungen in den Social Media eine gewisse Dynamik durch Funktionen wie das Teilen oder Liken. Sie erreichen damit ohne Aufwand eine Vielzahl von Personen.

Im Folgenden sollen die Aspekte Hate Speech und Fake News einer kurzen (straf-)rechtlichen Würdigung unterzogen werden. Hieran schließt sich eine Widmung des Netzwerkdurchsetzungsgesetzes (NetzDG), das die Verbreitung entsprechender Inhalte eindämmen soll, an. Schließlich wird sowohl die Notwendigkeit als auch die potentielle Ausgestaltung von Gegenmaßnahmen thematisiert.

II. Hate Speech unter strafrechtlichen Gesichtspunkten

Der Begriff Hate Speech spielt für die strafrechtliche Beurteilung nach deutschem Recht keine Rolle. Es gibt weder eine Legaldefinition noch einen Straftatbestand zur Ahndung dieser. Selbst wenn übereinstimmende Kriterien für das Vorliegen von Hate Speech existierten und eine konkrete Äußerung nach diesen Maßstäben als Hate Speech eingeordnet würde, kann also nicht automatisch auf eine Strafbarkeit der Äußerung geschlossen werden. Allerdings rücken regelmäßig bestimmte Delikte in den Fokus:

Beleidigung nach § 185 StGB[8], üble Nachrede nach § 186, Verleumdung nach § 187, üble Nachrede und Verleumdung gegen Personen des öffentlichen Lebens nach § 188, öffentliche Aufforderung zu Straftaten nach § 111 sowie Volksverhetzung, § 130.

---

7 Milker, ZUM 2017, S. 216, 218.

8 Alle im Folgenden genannten §§ ohne Gesetzesangaben sind solche des StGB in der Fassung vom 13.11.1998 BGBl. I S. 3322, zuletzt geändert durch Gesetz v. 30.10.2017 BGBl. I S. 3618.

1. Schutz der persönlichen Ehre

Die Straftatbestände der §§ 185, 186, 187 bewirken den Schutz der persönlichen Ehre.[9] Eine strafrechtliche Beurteilung im Rahmen dieser Delikte hängt in der Praxis oftmals entscheidend von der Abwägung zwischen der Meinungsfreiheit aus Art. 5 Abs. 1 S. 1 Fall 1 GG des Äußernden auf der einen und den Persönlichkeitsrechten des Betroffenen aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG auf der anderen Seite ab.[10] Erstere ist ein Kernbestandteil unseres Demokratieverständnisses und nimmt daher in Deutschland einen sehr wichtigen Stellenwert ein. Grundsätzlich ist das Äußern seiner Meinung, d.h. jedes Stellung beziehende Dafürhalten im Sinne einer präskriptiven Wertung, erlaubt. Dies gilt allerdings nicht schrankenlos, sondern findet seine Grenzen in den allgemeinen Gesetzen, zu denen auch die §§ 185-188 zählen. Deren Grundzüge sollen im Folgenden dargestellt werden.

a) § 185 – Beleidigung[11]

Tatbestandlicher Anknüpfungspunkt einer Beleidigung ist der Angriff auf die Ehre einer anderen Person durch Kundgabe von Nicht-, Gering- oder Missachtung.[12] Diese Kundgabe kann durch Äußerung von Tatsachen oder Werturteilen in wörtlicher, schriftlicher, bildlicher Art oder auch durch schlüssige Handlungen erfolgen.[13] Der Begriff der Ehre lässt sich nicht konturenscharf abgrenzen – vertreten wird heute jedoch überwiegend ein sog. dualistischer Ehrbegriff, nach dem sich Ehre als der aus einem sozialen Zuschreibungs- und Anerkennungsverhältnis entspringende Anspruch auf Achtung des Werts der Person definieren lässt.[14]

Dementsprechend komplex kann im Einzelfall auch die Bewertung sein, ob ein tatbestandlicher Ehrangriff vorliegt. So spielt beispielsweise das

---

9 § 187 umfasst in seiner 2. Var. zumindest nach herrschender Meinung auch den Vermögensschutz, auf den hier allerdings nicht eingegangen werden soll.

10 Vgl. auch Schönke/Schröder/Lencker/Eisele, § 193, Rn. 15.

11 Auf die Darstellung der Qualifikation des zweiten Halbsatzes – Begehung mittels einer Tätlichkeit – wird hier verzichtet.

12 Schönke/Schröder/Lencker/Eisele, § 185, Rn. 1; Fischer, § 185, Rn. 4.

13 Fischer, § 185, Rn. 5.

14 Fischer, vor § 185, Rn. 4.

soziale Umfeld, in dem die Aussage getätigt wird, eine nicht unerhebliche Rolle. Der Maßstab der Beurteilung ist dabei weder die Sicht des konkret Betroffenen, noch die des Täters, sondern beurteilt sich nach dem objektiven Sinngehalt.[15] Entscheidend ist also, wie ein durchschnittlicher Empfänger sie verstehen durfte. Das bloße Befinden als Beleidigung genügt folglich nicht – so sind etwa auch Unhöflichkeiten und Distanzlosigkeiten nicht strafbar. Dies lässt sich vor Allem mit der sog. Ultima-Ratio-Funktion des Strafrechts erklären.

Der Täter muss außerdem (bedingt) vorsätzlich handeln, d.h. er muss die Tatbestandsverwirklichung (hier die Ehrminderung) in Kenntnis der relevanten Umstände zumindest unter billigender Inkaufnahme für möglich halten. Eine zielgerichtete Absicht zur Kränkung muss seitens des Täters gerade nicht vorliegen.

Eine tatbestandsmäßige Beleidigung kann allerdings auch gerechtfertigt sein. Hier dürfte § 193 StGB den relevantesten Rechtfertigungsgrund im Rahmen der §§ 185 ff. darstellen. Der Täter macht sich demnach unter Umständen nicht strafbar, wenn er durch die Äußerung berechtigte Interessen wahrnimmt. Aus § 193 ergibt sich das Erfordernis einer Abwägung zwischen den Grundrechten des Äußernden und des Betroffenen[16] – beispielsweise der Meinungsfreiheit aus Art. 5 Abs. 1 S. 1 Fall 1 GG oder der Kunstfreiheit aus Art. 5 Abs. 3 Fall 1 GG – und dem Allgemeinen Persönlichkeitsrecht aus Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG.[17] Ein medienwirksames Beispiel für die Konfrontation dieser Grundrechte dürfte das mittlerweile eingestellte Strafverfahren gegen den Moderator eines Satire-Magazins (Jan Böhmermann) darstellen, der in einem Gedicht den türkischen Präsidenten Erdogan verbal anging.

b) § 186 – üble Nachrede

Vorausgesetzt wird das Behaupten oder Verbreiten einer Tatsache in Bezug auf einen anderen. Unter Behaupten ist das Hinstellen als nach eigener Überzeugung zutreffend gemeint; das Verbreiten definiert sich als

---

15 Schönke/Schröder/Lencker/Eisele, § 185, Rn. 8.

16 Schönke/Schröder/Lencker/Eisele, § 193, Rn. 1.

17 Vgl. Schönke/Schröder/Lencker/Eisele, § 193, Rn. 1, der von § 193 als einer Ausprägung der Grundrechte des Art. 5 GG spricht.

Mitteilung fremder Erkenntnisse oder Überzeugungen.[18] Die Tatsache muss ferner geeignet sein, den anderen in der Öffentlichkeit verächtlich zu machen oder herabzuwürdigen. Der Maßstab zur Beurteilung ist wie im § 185 objektiv. Zudem genügt die bloße Eignung zur Verächtlichmachung oder Herabwürdigung. Dass diese tatsächlich eingetreten ist, ist also nicht erforderlich.[19]

Eine weitere Voraussetzung der Strafbarkeit ist die Unwahrheit der Tatsache („[…], wenn nicht diese Tatsache erweislich wahr ist,[…]“).[20]

In subjektiver Hinsicht lässt sich grundsätzlich auf die Ausführungen des § 185 verweisen, erforderlich ist also ein zumindest bedingter Vorsatz des Täters. Angemerkt sei hier allerdings, dass sich dieser nach h.M. nicht auf die Unwahrheit der Tatsachenäußerung beziehen muss.

Bezüglich der Rechtswidrigkeit ist auch hier § 193 in den Blick zu nehmen. Die unter 2.1.a. getätigten Ausführungen gelten auch für § 186 – allerdings mit dem entscheidenden Unterschied, dass bei der Beurteilung gerade nicht Art. 5 Abs. 1 S. 1 Fall 1 GG zugunsten des Täters zu berücksichtigen ist. Denn § 186 erfasst allein die Äußerung von Tatsachen, die aber gerade nicht dem Schutzbereich der Meinungsfreiheit des Art. 5 Abs. 1 S. 1 Fall 1 GG unterfallen.

Schließlich enthält § 186 in seinem zweiten Halbsatz eine Qualifikation (Strafschärfung) für den Fall, dass die Tat öffentlich (Alt. 1) oder durch die Verbreitung von Schriften, Ton- oder Bildträgern, Abbildungen oder Darstellungen (Alt. 2) begangen wird, worauf sich der Vorsatz des Täters freilich ebenfalls beziehen muss. Bei Kundgabe entsprechender Inhalte in Foren, Kommentarbereichen, auf Social-Media-Plattformen oder Webseiten dürften beide Alternativen erfüllt sein. Für die Öffentlichkeit genügt die Möglichkeit zur Kenntnisnahme einer größeren, nicht durch nähere

---

18 Fischer, § 186, Rn. 8 f.

19 Bamberger et al./Varius, § 186, Rn. 8.

20 Umstritten, aber in der Sache unbedeutend ist, ob es sich dabei um ein Tatbestandsmerkmal oder um eine – so die herrschende Meinung – objektive Bedingung der Strafbarkeit handelt. Relevanz entfaltet die Einordnung nur bei der Beurteilung des subjektiven Tatbestands.

Beziehungen zueinander verbundenen Anzahl von Personen;[21] bei Äußerungen in Daten-Netzwerken sind die für schriftliche Äußerungen geltenden Grundsätze entsprechend heranzuziehen.[22]

c) §§ 187, 188 – Verleumdung, üble Nachrede und Verleumdung gegen Personen des politischen Lebens

Bei § 187 handelt es sich um eine Qualifikation (Strafschärfung) des Straftatbestandes der üblen Nachrede aus § 186. Aus diesem Grund wird größtenteils auf die entsprechenden Ausführungen verwiesen.

Im Unterschied zu § 186 muss sich der Vorsatz auch auf die Unwahrheit der Äußerungen beziehen. Zudem muss der Täter wider besseres Wissen handeln, d.h. positive Kenntnis bezüglich des Tatbestands, also insbesondere der Unwahrheit, gehabt haben.

Schließlich enthält der § 188 in Abs. 1 eine Qualifikation zur üblen Nachrede. Abs. 2 umfasst eine Qualifikation zur Verleumdung. Geschützt werden sollen damit im politischen Leben stehende Personen.

d) Verhältnis der §§ 185 – 187 untereinander

Wichtig für ein grundlegendes Verständnis des strafrechtlichen Ehrschutzes ist das Verhältnis der §§ 185 – 187 untereinander.[23] Grundsätzlich kann ein o.g. Angriff auf die Ehre, d.h. die Kundgabe von Nicht-, Gering- oder Missachtung entweder durch Mitteilung von Werturteilen oder aber von (unwahren oder wahren) Tatsachen erfolgen. Letztere unterscheiden sich von Werturteilen vereinfacht gesagt durch deren Beweisbar- bzw. Nachprüfbarkeit. Im Einzelnen kann die Unterscheidung jedoch sehr komplex sein; die Grenzen sind oftmals fließend. Insbesondere, wenn eine Aussage beide Elemente enthält, ist auf dessen überwiegenden Teil abzustellen.[24]

---

21 Schönke/Schröder/Lencker/Eisele, § 186, Rn. 19.

22 Fischer, § 186 Rn. 17, 19.

23 Hierbei sei angemerkt, dass die zu diesem Unterpunkt folgenden Ausführungen keineswegs unumstritten sind, sondern allenfalls dem „gängigen“ Meinungsstand entsprechen.

24 Fischer, § 186 Rn. 3.

§ 185 umfasst als Tathandlung die Äußerung von ehrmindernden Werturteilen gegenüber dem Tatopfer oder über das Tatopfer gegenüber Dritten. Bezüglich der Mitteilung ehrmindernder Tatsachen wird von § 185 nur eine solche unmittelbar gegenüber dem Tatopfer erfasst.

§ 186 ist dagegen einschlägig, wenn Tatsachen über das Tatopfer gegenüber Dritten geäußert werden, d.h. wenn Beleidigter und Empfänger der Aussage nicht personengleich sind.[25] § 187 ist schließlich eine Qualifikation des § 186 – und erfasst somit grundsätzlich die gleichen Konstellationen wie dieser.

e) Zwischenfazit

Basierend auf den vorgenannten Darstellungen lassen sich einige typische Situationen wie folgt einordnen. Tätigt jemand ehrverletzende Äußerungen über oder gegenüber einem anderen in für alle bzw. mehrere Personen einsehbaren virtuellen Räumen (beispielsweise der Kommentarbereich einer Nachrichtenmeldung, die Kommentierung von Social-Media-Beiträgen wie Facebook oder Twitter oder auf seiner eigenen, dort eingerichteten Profilseite), so unterfällt dies im Fall von Werturteilen dem Straftatbestand des § 185. Bedient sich der Täter in solchen Räumen Tatsachenbehauptungen, kommen die §§ 186 – 188 in Betracht.

Adressiert der Täter die ehrverletzenden Äußerungen etwa mittels einer privaten Nachrichtenfunktion bei Facebook oder per E-Mail unmittelbar an das Opfer, sodass Adressat des Inhalts allein der Betroffene selbst ist, so kommt lediglich eine Strafbarkeit nach § 185 in Betracht – unabhängig davon, ob es sich um ein Werturteil oder eine Tatsachenbehauptung handelt.

2. Öffentliche Aufforderung zu Straftaten

Für eine Strafbarkeit nach § 111 muss der Täter öffentlich (oder in einer Versammlung oder durch Verbreiten von Schriften) zu einer rechtswidrigen Straftat auffordern.[26] Die Erklärung muss auf ein bestimmtes Verhalten gerichtet sein und objektiv den Eindruck der Ernstlichkeit erwecken.

---

25 Vgl. Schönke/Schröder/Lencker/Eisele, § 186, Rn. 6.

26 Zum Merkmal der Öffentlichkeit siehe bereits 2.1.b.

Zudem muss sie sich an unbestimmt viele Menschen richten; die Aufforderung gegenüber einer Einzelperson genügt nicht.[27] Letztere dürfte vielmehr in den Anwendungsbereich des § 30 Abs. 1 fallen, der u.a. den Versuch einer Anstiftung zu einer Straftat erfasst. Weiterhin ist § 111 dahingehend restriktiv zu verstehen, als dass das bloße Gutheißen oder Befürworten nicht den Tatbestand erfüllt; entscheidend ist der Appellcharakter der Äußerung.[28] Nicht erforderlich ist, dass die Tat im Anschluss an die Aufforderung auch begangen wird, vgl. Abs. 2. In subjektiver Hinsicht genügt seitens des Täters der bedingte Vorsatz (zum bedingten Vorsatz vgl. o. 2.a.).

Bemerkenswert ist, dass die Norm in der Praxis trotz einem erhöhten Kommunikationsverkehr im Internet bislang keinen Bedeutungszuwachs verzeichnen konnte.[29]

3. Volksverhetzung

Der Straftatbestand des § 130 ist komplex gefasst und entzieht sich daher einer kurzen Darstellung. Genannt seien an dieser Stelle zur Veranschaulichung aber die Tathandlungen des Abs. 1. Dieser umfasst die Aufstachelung zum Hass und die Aufforderung zu Gewalt- oder Willkürmaßnahmen (Nr. 1) sowie die Beschimpfung, böswillige Verächtlichmachung oder Verleumdung (Nr. 2) in einer Weise, die zur Störung des öffentlichen Friedens geeignet ist. Die o.g. Handlungen müssen sich dabei gegen eine nationale, religiöse oder durch ihre ethnische Herkunft bestimmte Gruppe, gegen Teile der Bevölkerung oder gegen einen Einzelnen wegen seiner Zugehörigkeit zu einer der zuvor genannten Gruppen richten.

III. Rechtliche Einordnung von Fake News

Die – sogar gezielte – Verbreitung von Unwahrheiten an sich ist grundsätzlich nicht verboten, d.h. ist weder strafrechtlich sanktioniert, noch kann auf zivilrechtlicher Ebene dagegen vorgegangen werden.

---

27 Heintsche-Heinegg/Dallmeyer, § 111, Rn. 4.

28 Ostendorf/Frahm/Doege, NStZ 2012, S. 529, 532.

29 Vgl. Joecks/Miebach/Bosch, § 111, Rn. 4.

Etwas anderes kann aber gelten, wenn bestimmte Umstände hinzutreten. Wenn sich die Fake News auf andere, konkrete Personen beziehen und geeignet sind, diese herabzuwürdigen, kann dies beispielsweise nach den bereits unter 2.1 dargestellten Straftatbeständen der §§ 185 – 187 strafbar sein.[30] Die Beurteilung, wann eine solche Eignung zur Herabwürdigung anzunehmen ist, kann wiederum äußerst komplex sein und ruft bereits jetzt Debatten in der Rechtswissenschaft auf den Plan – so z. B. die Frage nach einem normativen oder faktischen Verständnis der Eignung zur Ehrverletzung. Anschaulich formuliert geht es dabei etwa um die Frage, ob die Behauptung, jemand sei homosexuell, das Tatbestandsmerkmal der Eignung zur Herabwürdigung bzw. dem Verächtlichmachen erfüllt. Homosexualität kann bei einem normativen Verständnis nicht ehrenrührig sein – faktisch wird dies leider auch heutzutage in manchen Teilen der Bevölkerung anders gesehen.[31]

Ein weiteres Beispiel für die potentielle Strafbarkeit von unwahren Äußerungen erst unter Hinzutreten weiterer Umstände, ist die Erregung von Irrtümern zur Erzielung von rechtswidrigen Vermögensvorteilen unter Schädigung des Vermögens anderer (Betrug, § 263). Ausnahmsweise kann in bestimmten Situationen jedoch bereits das Tätigen einer unwahren Aussage für sich genommen mit strafrechtlichen Konsequenzen versehen sein – dann aber auch nur in der Funktion eines Zeugen oder Sachverständigen vor Gericht. Hierzu kämen die Vorschriften der §§ 153 – 163 in Betracht.

Abseits des Strafrechts können insbesondere Ansprüche auf Schadensersatz, Geldentschädigung, Unterlassung, oder Gegendarstellung in Frage kommen. Nicht abschließend seien im Folgenden entsprechende Rechtsgrundlagen exemplarisch erwähnt.

---

30 Vgl. auch Hoven, ZStW 2017, S. 718, 719; hingewiesen sei auf die gelungene, nachfolgende Veranschaulichung der potentiellen Strafbarkeit von Fake News nach § 187 anhand der „Causa Künast“. Grünen-Politikerin Künast stellte anlässlich einer ihr angedichteten Äußerung, die in der Öffentlichkeit für Empörung sorgte, Strafanzeige wegen übler Nachrede (S. 721 ff.).

31 Angelehnt an Hoven, ZStW 2017, S. 718, 723.

1. § 823 Abs. 1 BGB

Gemäß § 823 Abs. 1 BGB kann bei rechtswidrigen und schuldhaften Eingriffen in das Allgemeine Persönlichkeitsrecht als sonstiges Recht i.S.d. § 823 Abs. 1 BGB vom Betroffenen Schadensersatz für hieraus entstandene materielle Schäden gefordert werden – beispielsweise der Gewinnausfall eines Restaurant-Betreibers, dessen Gäste aufgrund unwahrer Vorwürfe mangelnder Hygiene ausbleiben. Zwar bereitet die Beurteilung der Rechtswidrigkeit eines zurechenbaren Eingriffs in das Persönlichkeitsrecht oftmals Probleme, weil sie bei der Äußerung von Werturteilen von der Abwägung zwischen dem Persönlichkeitsrecht des Betroffenen aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG und der Meinungsfreiheit des Äußernden aus Art. 5 Abs. 1 S. 1 Fall 1 GG abhängt. Handelt es sich aber um unwahre Tatsachenbehauptungen, so unterfallen diese nicht dem Schutzbereich der Meinungsfreiheit (s.o.). Eine Rechtswidrigkeit dürfte damit im Regelfall vorliegen.

Liegen die o.g. Voraussetzungen vor, so besteht auch ein Anspruch auf den Widerruf der Äußerungen aus § 823 Abs. 1 BGB.

2. § 823 Abs. 1 BGB i.V.m. Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG

Liegt ein zurechenbarer, rechtswidriger und schuldhafter Eingriff in das Allgemeine Persönlichkeitsrecht vor, so kann neben dem Schadensersatz (s.o.) auch ein Geldentschädigungsanspruch verlangt werden.

3. § 824 BGB

Werden durch das rechtswidrige und schuldhafte Behaupten von unwahren Tatsachen die wirtschaftlichen Interessen eines anderen unmittelbar beeinträchtigt, so können sich auch aus § 824 BGB Ansprüche sowohl auf Schadensersatz als auch auf Widerruf der Aussage ergeben.

4. § 826 BGB

Selbiges ergibt sich auch aus § 826 BGB, wenn das Handeln als sittenwidrig zu qualifizieren ist und zusätzlich ein Schädigungsvorsatz seitens des Handelnden hinzukommt. Zur Annahme der Sittenwidrigkeit bedarf

es einer besonderen Verwerflichkeit der Handlung, die sich wiederum aus dem verfolgten Ziel, den eingesetzten Mitteln, der zu Tage tretenden Gesinnung oder den eingetretenen Folgen ergeben kann.[32] Regelmäßig erfasst sind vor diesem Hintergrund bewusst unrichtig erteilte Auskünfte.[33]

5. § 1004 Abs. 1 S. 2 BGB analog (i.V.m. § 823 Abs. 1 BGB)

Da § 823 Abs. 1 BGB für sich genommen nicht die zukünftige, drohende Verletzung des Allgemeinen Persönlichkeitsrechts schützt, besteht insoweit eine Schutzlücke, die über eine analoge Anwendung des § 1004 Abs. 1 S. 2 BGB geschlossen wird, sog. Quasinegatorischer Unterlassungsanspruch. Steht also ein rechtswidriger (nicht notwendigerweise schuldhafter) Eingriff in das Allgemeine Persönlichkeitsrecht mit hinreichender Wahrscheinlichkeit bevor, so hat der Betroffene einen Anspruch auf Unterlassung. Zwar setzt der Wortlaut des S. 2 hierfür voraus, dass in der Vergangenheit bereits eine Beeinträchtigung dessen stattgefunden haben muss („weitere Beeinträchtigungen“). Vor dem Hintergrund des effektiven Rechtsschutzes ist mittlerweile jedoch anerkannt, dass ein solcher Anspruch auch vor einer erstmaligen Beeinträchtigung bestehen kann.[34]

Zusammenfassend lässt sich also festhalten, dass zur Auslösung von rechtlichen Konsequenzen neben der bloßen Äußerung von Unwahrheiten grundsätzlich noch weitere Voraussetzungen hinzutreten müssen. Die obigen, keineswegs abschließenden Darstellungen zeigen, dass der hauptsächliche Anknüpfungspunkt in der Regel gerade nicht das Merkmal der Unwahrheit einer getätigten Aussage ist.

IV. Das NetzDG

Am 01.10.2017 in Kraft getreten, zielt das Netzwerkdurchsetzungsgesetz (kurz NetzDG) darauf ab, Hasskriminalität, strafbare Falschnachrichten und andere strafbare Inhalte auf den Plattformen sozialer Netzwerke

---

32 Bamberger et al./Förster, § 826 Rn. 19.

33 Bamberger et al./Förster, § 826 Rn. 75 f.

34 Bamberger et al./Fritzsche, § 1004 Rn. 78.

wirksamer zu bekämpfen.[35] Normadressaten sind offene soziale Netzwerke mit einer Mindestnutzerzahl von zwei Millionen in Deutschland. Im Wesentlichen statuiert das Gesetz für diese eine halbjährige Berichtspflicht über den Umgang mit Beschwerden über rechtswidrige Inhalte (§ 2 NetzDG), eine Pflicht zur Schaffung eines wirksamen und transparenten Verfahrens für den Umgang mit derartigen Beschwerden (§ 3 NetzDG) sowie eine Bußgeldbewehrung im Falle der Zuwiderhandlung (§ 4 NetzDG).

Große Kritik hat bereits im Vorfeld die Pflicht zur unverzüglichen Sperrung/Löschung rechtswidriger Inhalte[36] seitens des Netzwerkbetreibers hervorgerufen – in der Regel soll dies innerhalb von sieben Tagen nach Eingang einer Beschwerde geschehen (§ 3 Abs. 2 Nr. 3 NetzDG); bei offensichtlich rechtswidrigen Inhalten soll die Sperrung/Löschung innerhalb von 24 Stunden geschehen. Dabei wird zum einen die berechtigte Frage aufgeworfen, wie der jeweilige Netzbetreiber innerhalb weniger Tage – oder sogar Stunden – das leisten soll, wofür bei einem entsprechenden Vorfall in der „analogen Welt“ ansonsten ein unter Umständen komplexes gerichtliches Verfahren notwendig ist. So wird einem Bearbeiter des Medienportals in der Regel auch der Kontext der Äußerung verborgen bleiben – evtl. wurde der Autor eines potentiell rechtswidrigen Inhalts zuvor selbst persönlich scharf angegangen, was sich im Rahmen einer strafrechtlichen Beurteilung ganz erheblich auswirken kann. Es existiert ein sog. Recht zum Gegenschlag[37] – oder ganz profan formuliert: Wie man in den Wald hineinruft, so schallt es wieder heraus.

---

35 Siehe http://www.bmjv.de/DE/Themen/FokusThemen/NetzDG/NetzDG_node.html (zuletzt abgerufen: 11/2018).

36 Diese sind definiert in § 1 Abs. 3 NetzDG und umfassen die Verwirklichung des Tatbestands und Rechtswidrigkeit von diversen Strafgesetzen, etwa § 130, §§ 185-187 StGB.

37 Vgl. BVerfG, Beschluss vom 10.03.2016 – 1 BvR 2844/13. In jüngster Zeit hatte beispielsweise die Aussage „Sie sind ein wunderbares Inzuchtsprodukt“ des Herrn Schneider-Addae-Mensah, gerichtet an den bayrischen Innenminister Herrmann für Medienaufmerksamkeit gesorgt. Zwar läge hierin eine tatbestandsmäßige Beleidigung, diese sei jedoch vor dem Hintergrund voriger Äußerungen Herrmanns gerechtfertigt, so das LG Karlsruhe, Beschluss vom 20.07.2016 – 4 Qs 25/16. Der bayrische Innenminister Herrmanns hatte zuvor in einer Talkshow den Begriff „Neger“ verwendet und damit für Empörung gesorgt.

Natürlich wird durch den Netzbetreiber keine verbindliche Beurteilung getroffen, ob sich ein Nutzer strafbar gemacht hat, d.h. aufgrund dessen Einordnung werden auch keine strafrechtlichen Sanktionen ausgelöst. Auch ist ein privater Netzbetreiber nicht unmittelbar an das Grundgesetz gebunden, d.h. unabhängig vom NetzDG kann er grundsätzlich bis zu einem gewissen Grad selbst bestimmen und durch AGB ausgestalten, welche Inhalte auf seiner Plattform geäußert werden dürfen.

Das NetzDG als Gesetz ist jedoch ein legislativer Akt der Staatsgewalt, der sich am Grundgesetz messen lassen muss. Ein solches Gesetz, das aufgrund hoher Bußgeldandrohungen – wenngleich nicht intendiert – faktisch dazu führt, dass Private zu Löschungen nicht rechtswidriger, d.h. von der Meinungsfreiheit gedeckter Äußerungen, gedrängt werden, würde Art. 5 Abs. 1 S. 1 Fall 1 GG verletzen und wäre mithin verfassungswidrig.[38] Der Gesetzgeber kann sich auch nicht darauf berufen, dass die Lösch- bzw. Sperrpflicht nur für rechtswidrige Inhalte gilt, wenn zu erwarten ist, dass die Netzbetreiber zur Vermeidung von Bußgeldern in unklaren Fällen tendenziell auch (noch) rechtmäßige Inhalte löschen, sog. Overblocking.

Zwar ist an dieser Stelle anzumerken, dass der Anknüpfungspunkt der Bußgeldbewehrung nicht ein Verstoß gegen die Lösch-/Sperrpflicht einzelner Inhalte, sondern vielmehr die mangelnde Einrichtung, Organisation und Überwachung eines in § 3 NetzDG bezeichneten Verfahrens ist und dies die Gefahr eines Overblockings tatsächlich mindern dürfte. Beseitigt ist sie damit allerdings nicht.[39] Dies dürfte sich kürzlich öffentlichkeitswirksam bestätigt haben, als eine ganz offensichtlich satirische Äußerung des Satiremagazins „Titanic“ sowohl auf Facebook als auch auf Twitter gesperrt wurde.[40] Angemerkt sei schließlich, dass bereits vor Inkrafttreten des NetzDG eine Pflicht zur Löschung rechtswidriger Inhalte bestand – aus der sog. zivilrechtlichen Störerhaftung nach §§ 1004, 823

---

38 Zu einem entsprechenden Ergebnis gelangt beispielsweise Nolte, ZUM 2017, S. 552, 555. Nolte legt weiterhin zahlreiche andere Gründe für die Verfassungswidrigkeit des NetzDG dar.

39 Guggenberger, ZRP 2017, S. 98.

40 http://www.faz.net/aktuell/feuilleton/medien/twitter-sperrt-titanic-magazin-wegen-storch-satire-15371919.html (zuletzt abgerufen: 11/2018).

BGB, was zusätzlich die Frage nach der Erforderlichkeit des NetzDG aufwirft.

Auch auf europarechtlicher Ebene ist die Vereinbarkeit des NetzDG mit geltendem Recht umstritten. So wird beispielsweise angeführt, das NetzDG verstoße gegen die E-Commerce-Richtlinie, wonach die Haftung von Hostprovidern in Art. 14 erst ab Kenntnis und offenkundiger Rechtswidrigkeit bejaht wird.[41]

Ob sich das NetzDG in Zukunft bei einer – mit Sicherheit zu erwartenden – Prüfung durch das BVerfG behaupten kann, bleibt also abzuwarten.

V. Was tun?

Neben dem Netzwerkdurchsetzungsgesetz bestehen zahlreiche weitere Bestrebungen, Hate Speech und Fake News zumindest auf ein „erträgliches“ Maß einzudämmen.

Bezüglich der Bekämpfung von Hate Speech sei das sog. 12-Punkte-Programm des Bundesministeriums für Justiz und Verbraucherschutz zu erwähnen.[42] Unter anderem genannt wird dort die Verbesserung der strafrechtlichen Verfolgung und zu diesem Zweck Anpassungen von Nutzungsbedingungen von privaten Netzwerkbetreibern, die die Weitergabe von Nutzerdaten an die Strafverfolgungsbehörden gewährleisten.

Hinsichtlich der Breitenwirksamkeit begrenzt, aber doch sehr aufschlussreich über den Zusammenhang zwischen dem Sinken von Hemmschwellen und Anonymität im Internet, ist die Aktion der öffentlich-rechtlichen Medien „Sag´s mir ins Gesicht“.[43] Hier wird zu Nutzern, die in der Vergangenheit durch unsachliche Kritik – und auch strafbare Äußerungen – aufgefallen sind, ein Kontakt hergestellt. Per Videochat kommen diese dann mit den angegriffenen Journalisten direkt ins Gespräch. Es bestätigt sich, dass die in diesen Gesprächen von Angesicht zu Angesicht geäußerte

---

41 Hoeren, NJW-aktuell 2018, S. 15; Nolte, ZUM 2017, S. 552, 561.

42 http://www.fair-im-netz.de/WebS/NHS/DE/Home/home_node.html;jsessionid=C47DDF6B97EFBE9DC77777FC69CEE182.2_cid289#initiative((zuletzt abgerufen: 11/2018).

43 http://www.tagesschau.de/inland/sags-mir-ins-gesicht-115.html (zuletzt abgerufen: 11/2018).

Kritik die sachliche Ebene nicht verlässt, auch wenn freilich oftmals kein inhaltlicher Konsens gefunden wird.

Auch zur Eindämmung von Fake News existieren in etablierten Medien Projekte – so beispielsweise der Tagesschau-„Faktenfinder“, der aktuelle Entwicklungen und hierzu existierende, verzerrende Berichterstattungen oder sachlich falsche Aussagen unter die Lupe nimmt und richtig stellt. Allerdings sind auch diese Versuche z.T. berechtigter Kritik[44] ausgesetzt, wie ein Fall aus der Vergangenheit darlegt: Die AfD hatte 2017 auf einem Wahlplakat „gähnende Leere“ auf dem Oktoberfest beklagt – sinngemäß aufgrund verfehlter Einwanderungspolitik, die ihrem Urteil nach zu erhöhter Terrorgefahr geführt hatte. Der ARD-Faktenfinder warf der AfD daraufhin wortwörtlich „Falschaussagen“ vor und begründete dies damit, dass am ersten Oktoberfestwochenende 2017 rund 600.000 Besucher und damit 100.000 mehr als im Vorjahr erschienen. Diese vom Faktenfinder recherchierten Zahlen waren an sich zwar nicht zu beanstanden, ließen aber unberücksichtigt, dass im jahrzehntelangen Durchschnitt rund 900.000 Besucher das Oktoberfest am ersten Wochenende aufsuchen. Die Resonanz fiel unabhängig der Ursachen im Jahr 2017 im Gesamtkontext gesehen also tatsächlich erheblich geringer aus.

Entsprechende Ansätze wie der Faktenfinder können – bei objektiver Berichterstattung und Berücksichtigung des gesamten Kontextes – durchaus zumindest bezüglich einzelner, aktuell populärer Themen dazu beitragen, dem Einfluss von Fake News entgegenzusteuern. Auch wenn die Idee dahinter also sinnvoll und achtenswert ist, stellen solche Ansätze aber kein realistisches Gegengewicht zur Fülle von Falschmeldungen dar.

Der Erarbeitung von Maßnahmen, die genau dies bezwecken, hat sich allerdings die EU-Kommission mittlerweile gewidmet. Die von ihr eingesetzte Expertengruppe rät dazu, auf mehreren Ebenen tätig zu werden. Unter anderem erwähnt sei hier das Schaffen von Transparenz, die Stärkung von Medienkompetenz beim Nutzer und die kontinuierliche Forschung sowie Evaluation der Wirksamkeit von Gegenmaßnahmen.[45]

---

44 Siehe etwa http://www.faz.net/aktuell/feuilleton/medien/afd-macht-wahlkampf-mit-fake-news-vom-oktoberfest-15209905.html (zuletzt abgerufen: 11/2018).

45 Europäische Kommission, S. 35.

VI. Fazit

Zweifellos dürfte das Internet – also beispielsweise Kommentarbereiche, Foren, soziale Medien – der Ort sein, an dem sich die Phänomene Hate Speech und Fake News am deutlichsten wahrnehmen lassen. Drastischer formuliert könnte man auch sagen, dass Hate Speech und Fake News überhaupt erst aufgrund des Internets mittlerweile als gesamtgesellschaftliches Problem realisiert wurden.

Schaut man einmal hinter die beiden Begrifflichkeiten, so stecken dahinter, wie eingangs erwähnt, allerdings keine neuen Entwicklungen des digitalen Zeitalters.

So geht es bei Hate Speech hauptsächlich schlicht und einfach um das Tätigen von strafbaren Äußerungen. Möchte man entsprechende Inhalte unterbinden, ist das wirksamste Mittel, die Strafverfolgungsorgane mit den notwendigen Ressourcen auszustatten, um solche Delikte auch bei Begehung im virtuellen Raum konsequent zu ahnden. Wenn dem mit dem Argument begegnet wird, dies sei aufgrund der unüberschaubaren Anzahl an Kommunikationen im Internet wirtschaftlich nicht zu leisten, wird dabei eines vergessen: Die strafrechtliche Sanktion einzelner Übertritte hat bei entsprechender öffentlicher Wahrnehmung eine erhebliche Symbolwirkung für die Gesellschaft, d.h. sie wirkt generalpräventiv.

Was bleibt, sind jedoch die soziologischen Fragen nach den Ursachen. Ist die allgemeine Stimmung in der Gesellschaft tatsächlich aggressiver geworden? Ist die Gesellschaft tatsächlich intoleranter geworden? Lassen sich derartige Entwicklungen überhaupt empirisch ermitteln? Können Aufklärungskampagnen in Schulen oder den Medien dabei helfen, mehr Respekt im Netz zu erzeugen? Oder glauben wir nur unterbewusst, eine Verrohung der Diskussions- und Kommunikationskultur ausmachen zu können; und zwar, weil verbalen Übertritten aufgrund der schnellen Verbreitung durch das Internet heutzutage eine breitere Bühne geboten wird und wir sie deshalb besser wahrnehmen können?

Bei Maßnahmen gegen die Verbreitung von Unwahrheiten sollte – erwägt man gesetzliche Regelungen – insbesondere die Funktion des Strafrechts als ultima ratio berücksichtigt werden. Zudem bestehen bereits sowohl straf- als auch zivilrechtliche Regelungen beispielsweise für Fälle,

in denen die Verbreitung von Unwahrheiten Vermögensschäden oder Persönlichkeitsrechtsverletzungen nach sich zieht.

Besonders sinnvoll erscheint hier insbesondere ein (langfristig angedachter) Lösungsansatz, der sich zumindest auch mittelbar in den Empfehlungen der durch die EU-Kommission eingesetzten Expertengruppe wiederfindet: Die Adressaten von Fake News, also insbesondere Internetnutzer als Konsumenten von Online-Nachrichten, für die Problematik von Fake News zu sensibilisieren. In einem nächsten Schritt können diese dann idealerweise in die Lage versetzt werden, die Glaubwürdigkeit von Informationen im Netz selbst einzuschätzen oder wenigstens kritisch zu hinterfragen. Ganz konkret könnten hierfür Unterrichtsfächer in Schulen etabliert werden, die Kinder bereits frühzeitig mit dem Nutzen, aber auch den Gefahren des Internets vertraut machen.

Wichtig ist schließlich insgesamt, dass sich der Thematik rational genähert wird. Wird bei Gegenmaßnahmen nicht das notwendige Augenmaß angelegt, so stehen Nutzen und Schaden beispielsweise von gesetzlichen Regelungen schnell nicht mehr in einem angemessenen Verhältnis. Denn auch wenn Äußerungen, die in einem toleranten Weltbild von der Gesellschaft als nicht wünschenswert angesehen werden, durch das Informationszeitalter eine größere Erreichbarkeit zukommt: Eine Demokratie muss grenzwertige, aber von der Meinungsfreiheit gedeckte Äußerungen aushalten können. Ansätze, die zur Löschung nur potentiell rechtswidriger Inhalte führen, beschneiden mit der Meinungsfreiheit eines der wichtigsten Güter der Demokratie selbst.

In diesem Sinne sei an einen Ausspruch erinnert, der von Voltaire stammen soll: "I disapprove of what you say, but I will defend to the death your right to say it.“[46]

---

46 Evelyn Beatrice Hall schrieb Voltaire in ihrem Buch „The Friends of Voltaire“ eine entsprechende Aussage zu.

Literaturnachweise

Bamberger et al., Beck´scher Online-Kommentar BGB, 44. Edition 2017.

Europäische Kommission, A multi-dimensional approach to disinformation, https://ec.europa.eu/digital-single-market/en/news/final-report-high-level-expert-group-fake-news-and-online-disinformation/ (zuletzt abgerufen: 11/2018).

Fischer, StGB Kommentar, 63. Auflage München 2016.

Guggenberger, Das Netzwerkdurchsetzungsgesetz – schön gedacht, schlecht gemacht, ZRP 2017, S. 98-101.

Heintsche-Heinegg, Beck´scher Online-Kommentar StGB, 37. Edition 2018.

Hoeren, Sperrchaos, NJW-aktuell 2018, S. 15.

Hoven, Zur Strafbarkeit von Fake News – de lege lata und de lege ferenda, ZStW 2017, S. 718-744.

Joecks/Miebach, Münchener Kommentar StGB, Bd. 3, 3. Auflage München 2017.

Milker, Social Bots im Meinungskampf. ZUM 2017, S. 216-222.

Ministerkomitee des Europarats, Empfehlung Nr. R (97) 20 des Ministerkomitees an die Mitgliedstaaten über die „Hassrede“, http://www.egmr.org/minkom/ch/rec1997-20.pdf (zuletzt abgerufen: 11/2018).

Nolte, Hate-Speech, Fake-News, das „Netzwerkdurchsetzungsgesetz“ und die Vielfaltsicherung durch Suchmaschinen, ZUM 2017, S. 552-565.

Ostendorf/Frahm/Doege, Internetaufrufe zur Lynchjustiz und organisiertes Mobbing, NStZ 2012, S. 529-538.

Schönke/Schröder, StGB Kommentar, 29. Auflage München 2014.

Stefanowitsch, „Lies bloß nicht die Kommentare“ – Eine Einleitung, in der Broschüre „Geh sterben!“ – Hate Speech und Kommentarkultur im Internet, Amadeu Antonio Stiftung, https://www.amadeu-antonio-stiftung.de/hatespeech/geh-sterben-hate-speech-und-kommentarkultur-im-internet/ (zuletzt abgerufen: 11/2018).

E. Microtargeting – Gezielte Wähleransprache im Wahlkampf (Barbara Kolany-Raiser und Tristan Radtke)

Stand: Juli 2018

Abstract: Microtargeting

Mittels sog. Microtargeting soll Big Data den Parteien im Wahlkampf zu mehr Effizienz verhelfen. Der tatsächliche Einfluss auf Wahlergebnisse ist nicht empirisch belegt. Die gezielte Ansprache einzelner Wähler und Wählergruppen über soziale Netzwerke oder im datengestützten Haustürwahlkampf kam bereits bei der Bundestagswahl 2017 und deutlich intensiver in US-Wahlkämpfen zum Einsatz. Der Einsatz von Microtargeting wirft sowohl Fragen nach der demokratischen Legitimation durch Wahlen als auch insbesondere datenschutzrechtliche Fragestellungen auf. Die Datenschutz-Grundverordnung lässt Microtargeting nur unter strengen Voraussetzungen zu, wobei Parteien (mit-)verantwortlich für das durch sie durchgeführte Microtargeting sind.

I. Der datengestützte Wahlkampf

„Versprich allen alles."[1]

Schon in den Wahlkämpfen der Antike kam es darauf an, die einzelnen Wähler gezielt mit individuellen Versprechungen anzusprechen. Über 2000 Jahre später erreicht dies eine neue Dimension. Spätestens seit dem Wahlkampf Barack Obamas 2008 sind der datengestützte Wahlkampf und die gezielte Wähleransprache in aller Munde.[2] Auch acht

---

1 Philipp Freeman in der Zusammenfassung zu dem Ratgeber „Wie man eine Wahl gewinnt – Der antike Ratgeber" von Quintus Tullius Cicero.

2 Jungherr, Datengestützte Verfahren im Wahlkampf, S. 2.

Jahre später sorgte der US-Wahlkampf erneut für Aufmerksamkeit. In einem Bericht über den Wahlerfolg Donald Trumps wurde die Form der Datennutzung als eine neue Dimension beschrieben – als angeblich erfolgreichster Wahlkampfhelfer Trumps.[3] In dem Zusammenhang wurde später bekannt, dass Daten von weit über 50 Millionen Facebook-Nutzern Grundlage für Analysen von Cambridge Analytica waren.[4]

Im Zusammenspiel mit Big Data besteht das Potential, Wahlkämpfe durch zielgerichtete Wähleransprache und weitere Möglichkeiten zur Einflussnahme, wie etwa Social Bots[5], zu verändern. Auch in Deutschland wurde der Rückgriff auf Big Data im Rahmen des Bundestagswahlkampfs 2017 angeregt diskutiert. Die Parteien optimieren ihren Haustürwahlkampf[6] und schalten zielgerichtet Werbung auf sozialen Netzwerken wie Facebook.[7]

Im Rahmen des Microtargetings eröffnet sich den Parteien im Wahlkampf eine neue Dimension der zielgerichteten Wähleransprache. Beispielsweise hat die FDP im Jahr 2017 Interessenten des Streaming-Portals Netflix über Facebook-Werbeanzeigen mit Anspielungen auf das sog. Binge Watching[8] angesprochen, während Interessenten des US-Autobauers Tesla FDP-Anzeigen zum Thema „Mobilität der Zukunft“ gezeigt wurden.[9]

Diese neue Form des Wahlkampfs wirft sowohl ethische als auch rechtliche Fragen auf. Außerdem stellt sich die Frage, welchen Erfolg Big-Data-gestützte Methoden im Wahlkampf versprechen. Im Folgenden soll der

---

3 https://www.dasmagazin.ch/2016/12/03/ich-habe-nur-gezeigt-dass-es-die-bombe-gibt/ (zuletzt abgerufen: 11/2018).

4 https://www.zeit.de/2018/13/facebook-datenskandal-cambridge-analytica/komplettansicht (zuletzt abgerufen: 11/2018).

5 Siehe hierzu das Dossier „Big Data in Social Media & Wahlkampf“ (C.).

6 https://www.mdr.de/thueringen/cdu-app-wahlkampf-datenschutz-100.html (zuletzt abgerufen: 11/2018).

7 https://netzpolitik.org/2017/wahlkampf-in-der-grauzone-die-parteien-das-microtargeting-und-die-transparenz/ (zuletzt abgerufen: 11/2018).

8 Binge Watching meint das Schauen von mehreren Folgen einer Serie unmittelbar hintereinander.

9 https://netzpolitik.org/2017/wahlkampf-in-der-grauzone-die-parteien-das-microtargeting-und-die-transparenz/ (zuletzt abgerufen: 11/2018).

Mythos um Big Data im Wahlkampf insoweit gelüftet werden, als der Einsatz bei den Wahlkämpfen in den USA und in Deutschland analysiert wird, und die tatsächlichen und rechtlichen Grenzen des Microtargetings aufgezeigt werden.

II. Der Begriff des Microtargetings

Microtargeting wird in der Debatte oft als Buzzword für jedweden datengestützten Wahlkampf verwendet. Nach einer Definition ist Microtargeting die personalisierte und zielgerichtete Ansprache der einzelnen Wähler unter Vorhersage der Auswirkungen dieser Ansprache.[10] Als Subbegriff für die noch gezieltere Ansprache wird zum Teil „Nanotargeting" vorgeschlagen.[11] Unter dem recht weiten Begriffsverständnis können datengestützte Haustürwahlkämpfe ebenso wie gezielte Telefonanrufe oder personalisierte Werbeanzeigen im Internet als Microtargeting anzusehen sein. Das Element der gezielten und personalisierten Ansprache mittels gewonnener Daten ist zentral für Microtargeting.[12]

Selbst wenn sich die Ansprache nicht auf einzelne Wähler, sondern Wählergruppen – wie etwa im Bundestagswahlkampf 2017 – konzentriert, ist eine datenbasierte, zielgerichtete Ansprache dieser Wählergruppen von dem Begriff des Microtargetings aufgrund des prägenden Elements der zielgerichteten Ansprache erfasst. Die Erscheinungsformen des Microtargetings sind also vielfältig: Sei es etwa eine personalisierte Wahlkampf-Werbung auf Facebook aufgrund der Interessen des

---

10 Agan, Silent Marketing: Microtargeting.

11 Edsall, Let the Nanotargeting begin.

12 Barocas, The Price of Precision: Voter Microtargeting and Its Potential Harms to the Democratic Process, S. 31 ff.; Jungherr, Datengestützte Verfahren im Wahlkampf, S. 4; http://www.deutschlandfunk.de/digitale-kampagnenfuehrung-die-parteien-und-das-netz.724.de.html?dram:article_id=395541 (zuletzt abgerufen: 11/2018).

Nutzers[13] oder der Haustürwahlkampf in ausgewählten Hauszügen,[14] denen mit Hilfe der Datenanalyse eine Wahrscheinlichkeit der Parteiaffinität zugeordnet wird.

III. Für und Wider des Microtargetings

Microtargeting ist für die Parteien aufgrund seiner (potentiellen) Effizienzsteigerung äußerst interessant. Zum einen sollen die Wählergruppen ausfindig gemacht werden, deren Ansprache sich überhaupt lohnt. Es soll verhindert werden, Ressourcen für die Gewinnung von Wählern aufzuwenden, die ohnehin schon überzeugt sind oder nur mit unverhältnismäßigem Aufwand von der werbenden Partei zu überzeugen wären. Zum anderen sollen die so eingegrenzten Wähler mit den eingesetzten Mitteln zu einem möglichst großen Anteil von der eigenen Partei überzeugt werden. Diese gezieltere Ansprache und Mobilisierung unterschiedlicher Wähler kann zudem das Interesse der Wähler an Politik und Parteien fördern und ein Gefühl von Anerkennung und Bestätigung hervorrufen.

Letztlich soll Microtargeting aus Sicht der Parteien die Kosten für die Ansprache des einzelnen Wählers senken.[15] Das kann umso mehr gelingen, je mehr (korrekte) Daten über den einzelnen Wähler vorliegen und je genauer getroffene Prognosen anhand dieser Daten sind.[16] Im Zeitalter von Big Data, in dem immer mehr Daten, z. B. aus sozialen Netzwerken wie Facebook, zur Verfügung stehen, gewinnt der Einsatz von Microtargeting im Wahlkampf an Attraktivität. Obwohl sich aufgrund der zahlreichen Faktoren, die Einfluss auf das Wahlergebnis haben, die tatsächliche Wirksamkeit nicht ohne Weiteres messen lässt. Beispielhaft für einen missglückten Versuch der Effizienzsteigerung ist das Aufspüren von sog. Swing States, Bundesstaaten mit hauchdünnen Mehrheiten, im US-Wahl-

---

13 http://www.faz.net/aktuell/feuilleton/medien/big-data-im-wahlkampf-ist-micro targeting-entscheidend-14582735.html (zuletzt abgerufen: 11/2018).

14 http://politicaldatascience.blogspot.de/2017/08/fdpleaks-hype-und-hybris-im.html (zuletzt abgerufen: 11/2018).

15 Jungherr, Datengestützte Verfahren im Wahlkampf, S. 2 f.

16 http://politicaldatascience.blogspot.de/2017/08/fdpleaks-hype-und-hybris-im.html (zuletzt abgerufen: 11/2018).

kampf 2016. Man denke daran, dass Hillary Clinton im besagten Wahlkampf einzelne US-Bundesstaaten vernachlässigt hat – darunter auch Staaten, in denen Trump am Ende mit knapper Mehrheit obsiegte.

Unabhängig von der Frage nach der Effizienz und der rechtlichen Bewertung, kann Microtargeting weiteren Einfluss auf die Art des politischen Diskurses haben. Die klassischen Wahlkampfaktivitäten, wie etwa Auftritte von Politikern sowie Wahlwerbespots, konnten potentiell eine breite und heterogene Masse erreichen. Aus dem Grund haben auch Journalisten Zugang zu den Wahlkampf-Aussagen und ein breiter öffentlicher Diskurs ist möglich.

Soweit im Microtargeting dem einzelnen Wähler gezielt Versprechungen gemacht werden, ist ein Abgleich mit anderen Aussagen des gleichen Politikers nicht möglich. Widersprüche können nicht aufgedeckt und von einer breiten Öffentlichkeit erörtert werden. Microtargeting verstärkt also die Gefahr, dass womöglich widersprüchliche Versprechungen im Wahlkampf gar nicht öffentlich werden[17] und es leichter fällt, gezielt Wähler der konkurrierenden Parteien unentdeckt zu demobilisieren.[18] Auf langfristige Sicht müssten die Inhalte nicht einmal mehr von den Politikern selbst stammen. Schließlich sind in Zukunft auch von Algorithmen generierte Werbe-Inhalte denkbar, die gezielt auf den einzelnen Wähler zugeschnitten sind.[19] Letztlich entscheiden jedoch weiterhin Menschen darüber, ob und welche Inhalte und Botschaften ausgespielt werden sollen[20] bzw. welche Aufgaben von Algorithmen übernommen werden.

Je präziser das Microtargeting erfolgt, desto eher besteht die Möglichkeit, dass einzelne Gruppen gezielt im Wahlkampf vernachlässigt werden – mit womöglich negativen Folgen für die Wahlbeteiligung.[21] Andererseits kann

---

17 http://www.faz.net/aktuell/feuilleton/medien/big-data-im-wahlkampf-ist-micro targeting-entscheidend-14582735.html (zuletzt abgerufen: 11/2018).

18 http://www.sueddeutsche.de/digital/wahlkampf-in-sozialen-medien-koennen-parteien-mit-personalisierter-werbung-die-wahl-manipulieren-1.3581781 (zuletzt abgerufen: 11/2018).

19 Papakyriakopoulos et al., Informatik Spektrum 2017, S. 327, 333.

20 Heinrich Böll Stiftung, Microtargeting – digitales Marketing.

21 Barocas, The Price of Precision: Voter Microtargeting and Its Potential Harms to the Democratic Process, S. 33.

darin auch eine Chance bestehen, sog. Filterblasen[22] zu durchbrechen, indem potentielle Wähler der anderen Parteien mit gegensätzlichen Meinungen konfrontiert werden.[23]

Letztlich steht die Frage der demokratischen Legitimation im Mittelpunkt: Hilft Microtargeting den Wahlberechtigten, sich einen Überblick über unterschiedliche Meinungen zu verschaffen und führt es zu einer intensiveren Auseinandersetzung mit den Wahlen? Oder werden ausgewählte Wählergruppen verschreckt oder gar derart beeinflusst, dass sie keine freie Wahlentscheidung mehr treffen können?

Gerade hinsichtlich der US-Wahlkämpfe mit einer breiten Datenbasis und zahlreichen Prognosen wird vereinzelt daran gezweifelt, inwieweit diese Wahlen noch als geheim[24] und frei anzusehen sind.[25]

Wie so oft bei neuen technologischen Möglichkeiten eröffnet Microtargeting Chancen, birgt aber auch Risiken. Die Wählerschaft und ihre Wertvorstellungen können Einfluss darauf haben, wie das Microtargeting eingesetzt wird. Unter den Kritikern scheint sich jedenfalls ein Konsens herauszubilden: Microtargeting erfordert Transparenz.[26]

IV. Gezielte Wähleransprache in den USA

Insbesondere der Einsatz von Microtargeting in US-Wahlkämpfen offenbart seine Attraktivität für Parteien ebenso wie die unterschiedlichen Erscheinungsformen des Microtargetings.

---

22 Siehe hierzu das Dossier „Meinungsvielfalt im Big-Data-Zeitalter – die verfehlte Frage nach der Filterblase“ (B.).

23 Papakyriakopoulos et al., Informatik Spektrum 2017, S. 327, 334.

24 Papakyriakopoulos et al., Informatik Spektrum 2017, S. 327, 334.

25 Richter, DÖV 2013, S. 961, 969.

26 Barocas, The Price of Precision: Voter Microtargeting and Its Potential Harms to the Democratic Process, S. 34; Zuiderveen Borgesius et al., Utrecht Law Review 2018 (14), S. 82, 94; http://www.faz.net/aktuell/feuilleton/medien/big-data-im-wahlkampf-ist-microtargeting-entscheidend-14582735.html (zuletzt abgerufen: 11/2018); https://netzpolitik.org/2017/wahlkampf-in-der-grauzone-die-parteien-das-microtargeting-und-die-transparenz/ (zuletzt abgerufen: 11/2018).

Schon vor Obama setzte 2003 der Demokrat Howard Dean im Vorwahlkampf internetbasierte Kampagnen zur Wähleransprache ein.[27] In Vorbereitung auf den Wahlkampf bauten die Demokraten 2005-2007 eine umfassende, eigene Wählerdatenbank („Vote Builder“) auf und erleichterten zeitgleich die parteiinterne Organisation des Wahlkampfs durch eine neue parteiinterne Plattform.[28] Die Republikaner hingegen entwickelten vermutlich eine zuvor angelegte nationale Wählerdatenbank nach dem Wahlerfolg 2004 zunächst nur begrenzt weiter und waren den Demokraten damit zumindest auf diesem Feld unterlegen.[29] Als innovativ galt in Obamas Wahlkampf 2008 vor allem die präzise Vorhersage der Wahlergebnisse in den einzelnen US-Bundesstaaten, um die Swing States, in denen oft nur knappe Mehrheiten erzielt werden, zu erkennen.[30]

Der datenbasierte Wahlkampf wurde stetig optimiert. So wurde für den überraschenden Wahlerfolg Trumps 2016 ein entsprechender Erklärungsversuch unternommen: Mittels Daten von Facebook-Profilen soll es dem Unternehmen Cambridge Analytica gelungen sein, die Wertvorstellungen und politischen Einstellungen der Wahlberechtigten besser einzuschätzen, um das Wahlverhalten möglichst genau vorhersagen zu können.[31] Die Aktivitäten der Facebook-Nutzer seien so aussagekräftig, dass sich etwa anhand der Likes mit 95-prozentiger Wahrscheinlichkeit die Hautfarbe und mit 85-prozentiger Wahrscheinlichkeit die Parteiaffinität eines Nutzers vorhersagen lasse.[32] Ausschlaggebend sind damit – wie regelmäßig bei dem Einsatz von Big Data – auch bei diesem Verfahren Korrelationen, also Zusammenhänge zwischen verschiedenen Datensätzen.

---

27 Jungherr/Schoen, S. 69.

28 Jungherr/Schoen, S. 97.

29 Jungherr/Schoen, S. 98.

30 https://www.bigdata-insider.de/praesident-wird-wer-das-beste-data-science-team-hat-a-520504/ (zuletzt abgerufen: 11/2018).

31 https://www.dasmagazin.ch/2016/12/03/ich-habe-nur-gezeigt-dass-es-die-bombe-gibt/ (zuletzt abgerufen: 11/2018).

32 https://www.dasmagazin.ch/2016/12/03/ich-habe-nur-gezeigt-dass-es-die-bombe-gibt/ (zuletzt abgerufen: 11/2018). Siehe zu der Aussagekraft von Likes auch Dossier „Big Social Data“ (F.).

Die einfache Erklärung für den Wahlsieg Trumps wurde vielfach angezweifelt.[33] Im Jahr 2018 wurde publik, dass 87 Millionen Datensätze von Facebook-Nutzern die Grundlage für die Arbeit von Cambridge Analytica waren und entgegen der Facebook-Vorgaben genutzt wurden.[34] Dennoch fehlt es weiterhin an wissenschaftlichen Belegen für die Aussagekraft von Facebook-Profildaten über das Wahlverhalten eines Nutzers.[35]

Fest steht jedoch: In den USA spielen datengestützte Wahlkämpfe eine wichtige Rolle – auch wenn die tatsächlichen Auswirkungen einer einzelnen Methode auf das Wahlergebnis nur schwer zu messen sind.[36]

Ein Grund für die Bedeutung der datengestützten Wahlkämpfe ist die einzigartige Datengrundlage der Parteien. In den USA gibt es kein zentrales Einwohnermeldeamt. Zur Verhinderung von Wahlbetrug werden stattdessen öffentliche Wählerlisten („Voter Files“) geführt,[37] die von den US-Bundesstaaten an die Parteien weitergegeben werden.[38] Der Umfang der Datensätze divergiert je nach Bundesstaat, zum Teil sind auch Informationen über die ethnische Zugehörigkeit und die Registrierung zu den Vorwahlen der Demokraten oder aber der Republikaner enthalten.[39] Die Datensätze aus den Wählerverzeichnissen können um weitere Daten ergänzt werden, sodass sich noch umfangreichere Profile der Wahlberech-

---

33 Confessore/Hakim, Data firm says ‘secret sauce’ aided Trump; http://www.zeit.de/digital/internet/2016-12/us-wahl-donald-trump-facebook-big-data-cambridge-analytica (zuletzt abgerufen: 11/2018); http://www.spiegel.de/netzwelt/netzpolitik/donald-trump-und-die-daten-ingenieure-endlich-eine-erklaerung-mit-der-alles-sinn-ergibt-a-1124439.html (zuletzt abgerufen: 11/2018).

34 https://netzpolitik.org/2018/cambridge-analytica-was-wir-ueber-das-groesste-datenleck-in-der-geschichte-von-facebook-wissen/ (zuletzt abgerufen: 11/2018).

35 Jungherr, Datengestützte Verfahren im Wahlkampf, S. 13.

36 Siehe hierzu ausführlich: Pentzold/Fölsche, ABIDA-Gutachten „Die öffentliche Verhandlung von Big Data in politischen Kampagnen“, http://www.abida.de/sites/default/files/ABIDA%20Abschlussbericht%20Digitaler%20Demos.pdf, S. 27 ff., 36 ff.

37 Barocas, The Price of Precision: Voter Microtargeting and Its Potential Harms to the Democratic Process, S. 32.

38 Jungherr, Datengestützte Verfahren im Wahlkampf, S. 5.

39 Jungherr, Datengestützte Verfahren im Wahlkampf, S. 13.

tigten aus den Wählerlisten ergeben. Zu diesem Zweck kaufen die Demokraten und Republikaner z. B. Marketing-Daten ein.[40] Ergänzend werden Telefonbefragungen und Haustürgespräche geführt. Alleine im Verlauf von Obamas Kampagne 2012 gab es 120 Millionen Telefonkontakte.[41] Die Datenbank wurde so um zusätzliche Datensätze angereichert. Auf Grundlage aller gesammelten Daten lassen sich mit entsprechender Analyse-Software Zusammenhänge bzw. Korrelationen zwischen Verhalten, Interessen und Eigenschaften der Wahlberechtigten und ihrem Wahlverhalten ermitteln.[42]

Drei entscheidende Merkmale eines jeden Wähler-Profils im Wahlkampf 2012 waren der Grad der Unterstützung für Obama, gegebenenfalls die Wahrscheinlichkeit den Wahlberechtigten von Obama zu überzeugen und generell die Bereitschaft zu wählen.[43] Die Analyse ermöglichte die Konzentration der Wahlkampfressourcen, sodass mit den vorhandenen Mitteln möglichst große Effekte erzielt werden konnten.

Die Masse an verfügbaren Datensätzen und die langjährige Erfahrung der Wahlkämpfer in den USA ermöglichen die gezielte Wähleransprache in einer Dimension, wie sie beispielsweise in Deutschland derzeit kaum vorstellbar ist. Aus den vergangenen US-Wahlkämpfen lassen sich dennoch keine Rückschlüsse auf die Wirksamkeit von Microtargeting ziehen. Wobei sich eines zeigt: Fehlentscheidungen im Rahmen einer (Microtargeting-) Kampagne könnten verheerende Auswirkungen haben. Beispielsweise setzte Hillary Clinton im Wahlkampf 2016 auf ihren sicheren Sieg in einigen Staaten wie Michigan und Pennsylvania und vernachlässigte diese im Wahlkampf[44] – das Wahlergebnis und der Gewinner der Wahl sind bekannt.

---

40 https://www.bigdata-insider.de/praesident-wird-wer-das-beste-data-science-team-hat-a-520504/ (zuletzt abgerufen: 11/2018).

41 https://www.computerwoche.de/a/wie-obama-die-wahl-gewann,2539909 (zuletzt abgerufen: 11/2018).

42 Barocas, The Price of Precision: Voter Microtargeting and Its Potential Harms to the Democratic Process, S. 31 ff.

43 https://www.computerwoche.de/a/wie-obama-die-wahl-gewann,2539909 (zuletzt abgerufen: 11/2018).

44 Jungherr, Datengestützte Verfahren im Wahlkampf, S. 4.

V. Microtargeting in deutschen Wahlkämpfen

Deutschen Wahlkämpfern stehen bei Weitem keine Datensätze in einem solchen Umfang zur Verfügung. Dennoch versucht man hierzulande Wahlkampfbudgets dank datengestützter Prognosen und gezielter(er) Wähleransprache effizienter zu nutzen.

Im Bundestagswahlkampf 2017 kündigten die Parteien bereits vorab an, insgesamt mehrere Millionen Euro in den digitalen Wahlkampf investieren zu wollen.[45] Letzterer erschöpft sich zwar nicht in personalisierten Anzeigen auf sozialen Netzwerken und Suchmaschinen. Allerdings gehörten insbesondere die ca. 20 Millionen deutschen Facebook-Nutzer zu den stark umworbenen Zielgruppen.[46]

1. Microtargeting über soziale Netzwerke

Im Mittelpunkt des Microtargetings über soziale Netzwerke stand aufgrund dieser großen Zielgruppe daher auch Facebook. Werbeanzeigen auf Facebook lassen sich gezielt ausgewählten Nutzergruppen anzeigen. Diese Nutzergruppen können anhand demografischer Merkmale wie Alter und Geschlecht und anhand Interessen und Verhalten der Benutzer abgesteckt werden. So hat sich etwa die FDP im Bundestagswahlkampf 2017 gegenüber Nutzern mit Interesse an dem Thema Ausbildung als Bildungspartei präsentiert,[47] während der CDU-Politiker Jens Spahn mit einer Anzeige potentiellen AfD-Wählern gegenüber für „sichere Außengrenzen“ geworben hat.[48] Die AfD warb auf Facebook um Nutzer, die sich für den US-Präsidenten Trump interessieren.[49] Bündnis 90/Die Grünen

---

45 https://www.morgenpost.de/politik/article209403515/Wie-die-Parteien-2017-in-den-digitalen-Wahlkampf-ziehen.html (zuletzt abgerufen: 11/2018).

46 http://www.sueddeutsche.de/digital/wahlkampf-in-sozialen-medien-koennen-parteien-mit-personalisierter-werbung-die-wahl-manipulieren-1.3581781 (zuletzt abgerufen: 11/2018).

47 https://twitter.com/JKarthaeuser/status/896258852500512768 (zuletzt abgerufen: 11/2018).

48 https://twitter.com/DasErste/status/892293084347850752 (zuletzt abgerufen: 11/2018).

49 http://www.sueddeutsche.de/digital/wahlkampf-in-sozialen-medien-koennen-parteien-mit-personalisierter-werbung-die-wahl-manipulieren-1.3581781 (zuletzt abgerufen: 11/2018).

setzten sich für eine stärkere Anerkennung von Menschen in sozialen Berufen ein – mit Werbeanzeigen gezielt gegenüber Menschen in diesen Berufen.[50] Die beschriebenen Facebook-Anzeigen zeigen exemplarisch, dass sich auch die deutschen Parteien an den datengestützten, personalisierten Wahlkampf herantasten.

Vereinzelt sollen auch sog. Dark Posts zum Einsatz gekommen sein. Während klassische Werbeanzeigen auf Facebook der Promotion öffentlicher Beiträge dienen, sind Dark Posts nur für die ausgewählten Zielgruppen sichtbar, da sie nicht zeitgleich auf dem Profil der werbenden Facebook-Seite angezeigt werden.[51] Um diesem Phänomen zu begegnen, aber auch um bei klassischen Werbeanzeigen für mehr Transparenz zu sorgen, wurde der Hashtag „#PolitikAds“ ins Leben gerufen, unter dem Nutzer des Kurznachrichtendienstes Twitter die ihnen angezeigten Werbeanzeigen veröffentlichten.[52] Einzelne Parteien reagierten mit einer Transparenzoffensive und veröffentlichten alle bei Facebook geschalteten Werbeanzeigen an zentraler Stelle.[53]

Die sozialen Netzwerke Facebook[54] und Twitter[55] haben, wohl in Reaktion auf den US-Wahlkampf, in Zukunft mehr Transparenz bei Wahlwerbung zugesichert.

2. Datengestützter Haustürwahlkampf

Eine weitere Form der gezielten Wähleransprache wurde im Rahmen des Haustürwahlkampfs für die Bundestagswahl 2017 praktiziert. Die CDU

---

50 http://www.sueddeutsche.de/digital/wahlkampf-in-sozialen-medien-koennen-parteien-mit-personalisierter-werbung-die-wahl-manipulieren-1.3581781 (zuletzt abgerufen: 11/2018).

51 https://netzpolitik.org/2017/wahlkampf-in-der-grauzone-die-parteien-das-micro targeting-und-die-transparenz/ (zuletzt abgerufen: 11/2018).

52 https://twitter.com/wahl_beobachter/status/878923597175238656 (zuletzt abgerufen: 11/2018).

53 http://www.gruene.de/ueber-uns/2017/online-marketing-transparent.html (zuletzt abgerufen: 11/2018).

54 https://www.heise.de/newsticker/meldung/Facebook-Transparenz-Update-fuer-Wahlwerbung-3875608.html (zuletzt abgerufen: 11/2018).

55 https://www.tagesschau.de/ausland/twitter-transparenz-101.html (zuletzt abgerufen: 11/2018).

setzte dazu auf die hauseigene Smartphone-App Connect17, die aufgrund der Erfahrungen vergangener Wahlkämpfe stets weiterentwickelt wurde.[56] Eine Datengrundlage ist eine Potential-Analyse der Deutsche Post Direkt GmbH mit der statistischen Wahrscheinlichkeit, inwieweit im Rahmen eines Wohnblocks die CDU gewählt wird.[57] Daneben fließen alte Wahlergebnisse in die Analyse ein.[58] Die Smartphone-App sammelt Feedback der Wahlhelfer zu Haustür-Besuchen und versucht die Wahlhelfer durch Punkte und Ranglisten zu motivieren.[59] Die CDU-App war bereits Gegenstand von Untersuchungen der Datenschutzbeauftragten in Thüringen und Berlin,[60] ohne dass allerdings, soweit ersichtlich, Sanktionen verhängt wurden. Die CDU selbst betont stets, Daten nur bezogen auf Straßenzüge, nicht aber auf einzelne Haushalte zu erheben,[61] um so einen Personenbezug der Daten – welcher von Bedeutung für die Anwendbarkeit des Datenschutzrechts ist – auszuschließen.

Auch von anderen Parteien, wie etwa der SPD, ist bekannt, dass sie Haustür-Besuche bzw. das Feedback der potentiellen Wähler zusammengefasst in Haushaltseinheiten oder Straßenzügen protokollieren.[62] Bündnis 90/Die Grünen unterstützt die eigenen Wahlkämpfer ebenfalls mit einer Smartphone-App, um die Reaktionen auf einzelne Haustür-Besuche zu protokollieren – wobei unklar ist, ob tatsächlich, wie auf den Beispielfotos dargestellt, einzelne Hausnummern gespeichert werden.[63] Wahlkampf-Helfern der FDP stand ein Portal zur Verfügung, um die

---

56 https://www.mdr.de/thueringen/cdu-app-wahlkampf-datenschutz-100.html (zuletzt abgerufen: 11/2018).

57 https://netzpolitik.org/2017/wahlkampf-in-der-grauzone-die-parteien-das-microtargeting-und-die-transparenz/ (zuletzt abgerufen: 11/2018).

58 http://www.rp-online.de/nrw/landespolitik/big-data-im-wahlkampf-eine-app-hilft-der-cdu-beim-klinken-putzen-aid-1.6782424 (zuletzt abgerufen: 11/2018).

59 https://www.connect17.de/app/ (zuletzt abgerufen: 11/2018).

60 https://www.mdr.de/thueringen/cdu-app-wahlkampf-datenschutz-100.html (zuletzt abgerufen: 11/2018).

61 http://www.deutschlandfunk.de/digitale-kampagnenfuehrung-die-parteien-und-das-netz.724.de.html?dram:article_id=395541 (zuletzt abgerufen: 11/2018).

62 http://www.rp-online.de/nrw/landespolitik/big-data-im-wahlkampf-eine-app-hilft-der-cdu-beim-klinken-putzen-aid-1.6782424 (zuletzt abgerufen: 11/2018).

63 https://play.google.com/store/apps/details?id=de.gruene.greenapp&hl=de (zuletzt abgerufen: 11/2018).

Wahrscheinlichkeit für FDP-Wähler in einzelnen Straßen auf Grundlage verschiedener Daten zu ermitteln.[64]

Der datengestützte Haustürwahlkampf scheint somit zur Normalität zu werden. Im Mittelpunkt des Bundestagswahlkampfes 2017 stand dabei insbesondere die Sortierung nach Parteipräferenzen: Anhand soziodemografischer Daten, Daten aus vergangenen Wahlen und dem Feedback aus den Haustür-Besuchen, versuchten die Parteien Straßenzüge auszumachen, in denen sich der Haustürwahlkampf besonders lohnen könnte.

3. Fazit zu Microtargeting in deutschen Wahlkämpfen

Anhand des Wahlergebnisses der Bundestagswahl 2017 lassen sich keine Aussagen zu dem Erfolg des Microtargetings treffen. In anderen Wahlkämpfen soll der datengestützte Haustürwahlkampf hingegen bereits zu messbaren Stimmengewinnen geführt haben,[65] wobei auch in diesem Fall andere Faktoren ebenso maßgeblich gewesen sein könnten.

Tatsächlich versuchen alle großen Parteien ihren Wahlkampf mittels Microtargeting auf Effizienz zu trimmen. Während es den Parteien gelingt, zielgenau einzelne Wähler über Online-Werbekampagnen anzusprechen, helfen im Haustürwahlkampf grobe, datengestützte Analysen, um die jeweils aus Wahlkampf-Sicht interessanten Gebiete auszumachen. Mittlerweile stehen den Parteien dabei immer ausgereiftere Produkte zur Verfügung – wie das Beispiel der Connect17-App der CDU zeigt, die bereits über mehrere Landtags- und Bundestags-Wahlkämpfe hinweg eingesetzt wurde.

---

64 http://politicaldatascience.blogspot.de/2017/08/fdpleaks-hype-und-hybris-im.html (zuletzt abgerufen: 11/2018).

65 http://www.rp-online.de/nrw/landespolitik/big-data-im-wahlkampf-eine-app-hilft-der-cdu-beim-klinken-putzen-aid-1.6782424 (zuletzt abgerufen: 11/2018).

VI. Rechtliche Grenzen des Microtargetings in Deutschland

Das deutsche und europäische Datenschutzrecht setzt klare Grenzen für Microtargeting. Seit dem 25.05.2018 gilt die Datenschutz-Grundverordnung (DS-GVO[66]) unmittelbar in jedem Mitgliedstaat. Sie hat damit die EU-Datenschutz-Richtlinie 95/46/EG mit Umsetzungsvorschriften wie dem BDSG a.F. abgelöst.

Speziellere Regelungen, wie etwas das deutsche TMG, werden durch die Verordnung verdrängt.[67] Es bleibt abzuwarten, ob und wann stattdessen die geplante ePrivacy-Verordnung mit bereichsspezifischen Regelungen für Datenschutz im Rahmen elektronischer Kommunikationsdienste in Kraft tritt.[68]

Der deutsche Gesetzgeber hat von Öffnungsklauseln in der DS-GVO durch das Bundesdatenschutzgesetz vom 30.06.2017 mit Geltung seit dem 25.05.2018 (BDSG 2018) Gebrauch gemacht.

Im Wahlkampf kommt es entscheidend darauf an, ob der Anwendungsbereich der DS-GVO überhaupt eröffnet ist. Andernfalls sind auch etwaige Anforderungen an Erlaubnistatbestände und Datenschutz-Grundsätze nicht zu beachten.

1. Anwendbarkeit der DS-GVO in sachlicher Hinsicht und Verantwortlichkeit

Der sachliche Anwendungsbereich der DS-GVO umfasst nach Art. 2 DS-GVO nahezu jede (teil-)automatisierte Verarbeitung personenbezogener Daten. Nach Art. 4 Nr. 1 DS-GVO sind personenbezogene Daten Informationen, die sich auf eine identifizierte oder identifizierbare natürliche

---

66 Soweit nachfolgend Erwägungsgründe zitiert werden, sind dies solche der DS-GVO.

67 Plath/Hullen/Roggenkamp, Einleitung, Rn. 13.

68 Kommissionsentwurf vom 10.01.2017 in deutscher Sprache abrufbar unter: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=42678 (zuletzt abgerufen: 11/2018). Aktueller Entwurf vom 12.06.2018 in englischer Sprache: https://www.bvdw.org/fileadmin/bvdw/upload/dokumente/recht/e_privacy_verordnung/Entwurf_Text_ePrivacy_12.06.2018.pdf (zuletzt abgerufen: 11/2018).

Person beziehen. Dabei bleibt unklar,[69] ob es darauf ankommt, ob die verantwortliche Stelle (subjektive Perspektive) oder irgendein Dritter den Personenbezug herstellen kann (objektive Perspektive). In Bezug auf Microtargeting und Szenarien wie die Zuordnung von Wahrscheinlichkeiten zu einzelnen Haushalten oder Straßenzügen und zielgerichteten Wahlkampagnen über soziale Netzwerke kann diese Frage dahinstehen, soweit nicht etwa Kennungen wie IP-Adressen betroffen sind.[70] Der Begriff der Verarbeitung ist weit zu verstehen und umfasst nach Art. 4 Nr. 2 DS-GVO jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten.

Für präzises Microtargeting, wie es in den USA zum Teil bereits praktiziert wird, sind Daten zu möglichst jedem einzelnen Wähler unerlässlicher Bestandteil für genaue Prognosen. Das Anlegen solcher Profile in deutschen Wahlkämpfen, die beispielsweise anhand des Namens, der Angabe eines Facebook-Profils oder einer genauen Adressangabe, leicht einem einzelnen Wähler zugeordnet werden können, unterfällt dem Begriff der personenbezogenen Daten. Ebenso stellt die Weitergabe von Daten über einzelne Wahlberechtigte, etwa durch den „Einkauf“ von Marketing-Profilen wie bei Payback,[71] einen separaten Verarbeitungsvorgang dar.

Für die erwähnten Untersuchungen der Connect17-App durch Datenschutzbeauftragte war wieder einmal die Frage nach der Anwendbarkeit des Datenschutzrechts von Relevanz. Laut Auskunft der App-Entwickler würden Erfahrungen der Haustür-Wahlkämpfer nur unter Angabe des Straßennamens und ohne Hausnummer gespeichert.[72] Soweit präzisere Daten aufgenommen würden, erfolge dies nur mit der Einwilligung der

---

69 Kühling/Buchner/Klar/Kühling, Art. 4 Nr. 1, Rn. 26; Plath/Schreiber, Art. 4, Rn. 9 f.

70 EuGH, Urteil vom 19.10.2016 – C-582/14 – Breyer.

71 http://www.faz.net/aktuell/feuilleton/wie-big-data-das-wahlgeheimnis-aushebelt-wir-wissen-wen-du-waehlen-wirst-12553613.html (zuletzt abgerufen: 11/2018).

72 https://www.mdr.de/thueringen/cdu-app-wahlkampf-datenschutz-100.html (zuletzt abgerufen: 11/2018).

entsprechenden Betroffenen,[73] die sowohl nach § 4 Abs. 1 BDSG a.F. als auch nach Art. 6 Abs. 1 UA 1 lit. a, Art. 7 DS-GVO möglicher Erlaubnistatbestand ist.

Auch andere Parteien wie die FDP bemühen sich penibel, den Personenbezug zu vermeiden. Das unbeabsichtigt zeitweise für jedermann zugängliche Wahlkampf-Portal der Partei gab beispielsweise die Wahrscheinlichkeit der Wahl der FDP nur gebündelt für sechs zusammengefasste Gebäude an.[74]

Im Rahmen des Microtargetings sind insbesondere die Wahrscheinlichkeit, eine entsprechende Partei zu wählen und soziodemografische Daten wie das Haushaltsnettoeinkommen sowie Erfahrungen der Haustür-Wahlkämpfer von Bedeutung. Soweit von vornherein nur mit Daten gearbeitet wird, die mehreren Haushalten als eine Einheit zugeordnet werden, ist im Regelfall aufgrund der Anonymisierung keine Zuordnung zu einer einzelnen Person möglich und die DS-GVO kommt nicht zur Anwendung. Anders ist die Situation zu bewerten, soweit in einem Zwischenschritt Daten zu einzelnen Wahlberechtigten erhoben und anschließend zusammengeführt werden oder beispielsweise mehrere Haushalte zufällig einer einzigen natürlichen Person zuzuordnen wären. Der Balanceakt der deutschen Parteien zwischen möglichst genauen Daten und Nichtanwendbarkeit des Datenschutzrechts scheint also im Haustürwahlkampf zu gelingen. Eigens angelegte Wählerprofile, wie in den US-Wahlkämpfen, unterlägen hingegen der DS-GVO.

Die noch gezieltere Ansprache auf Grundlage erhobener Daten via Facebook erfolgt bereits intensiv durch deutsche Parteien. Die Datenverarbeitung durch Facebook wurde durch mehrere Datenschutzbehörden, darunter die französische, belgische und niederländische, untersucht und führte teilweise zur Verhängung von Bußgeldern.[75]

---

73 https://www.mdr.de/thueringen/cdu-app-wahlkampf-datenschutz-100.html (zuletzt abgerufen: 11/2018).

74 http://politicaldatascience.blogspot.de/2017/08/fdpleaks-hype-und-hybris-im.html (zuletzt abgerufen: 11/2018).

75 https://netzpolitik.org/2017/franzoesische-datenschutzbehoerde-verhaengt-hoechststrafe-gegen-facebook/ (zuletzt abgerufen: 11/2018).

Unabhängig von der Verantwortlichkeit Facebooks haben die Parteien, soweit sie Werbung über Facebook betreiben, selbst keinen weitergehenden Zugriff auf die Daten der Angesprochenen. Die Parteien legen jedoch über die Inhalte und Aktivitäten auf der beworbenen Fanpage und über die Einstellungen für die Werbeanzeigen das Zielpublikum fest und erhalten Zugriff auf anonymisierte Statistiken über den Erfolg von Fanpage und Werbeanzeigen. Da nach Art. 4 Nr. 7 DS-GVO bereits eine Entscheidung zusammen mit anderen über Zwecke und Mittel der Verarbeitung ausreichend ist, sind die Parteien für die Verarbeitung anlässlich ihrer Fanpages und Werbeanzeigen ebenfalls Verantwortliche im Sinne des Art. 4 Nr. 7 DS-GVO. Die Entscheidung des EuGH[76] zu der Verantwortlichkeit nach der Datenschutz-Richtlinie lässt sich insoweit auf die DS-GVO übertragen. Der Grad der Verantwortlichkeit von Facebook als Plattform-Betreiber und den Parteien bestimmt sich für die einzelnen Verarbeitungsphasen nach den Umständen des Einzelfalles.[77] Bereits eine Mitverantwortlichkeit für Verstöße kann etwa zur Durchführung von Maßnahmen der Aufsichtsbehörden, vgl. Art. 58 DS-GVO, oder zur Verhängung eines Bußgeldes führen, wenngleich der Grad der Verantwortlichkeit etwa nach Art. 83 Abs. 2 lit. d DS-GVO zu berücksichtigen ist.

Eine unveränderte Nutzung von Facebook als Microtargeting-Instrument in kommenden Wahlkämpfen kann also auch für die Parteien Folgen mit sich bringen. Das gilt zumindest soweit Facebook mit der Gestaltung seiner Plattform gegen die DS-GVO verstößt.

Zusammengefasst unterfällt der datengestützte Haustürwahlkampf der Parteien insoweit nicht der DS-GVO, als Haushaltseinheiten ohne Rückschlüsse auf einzelne natürliche Personen zusammengefasst werden. Noch ungeklärt ist die Bewertung und gegebenenfalls Sanktionierung der Werbemöglichkeiten bei Facebook, wobei die Parteien als Werbende zumindest mitverantwortlich sind.

---

76 EuGH, Urteil vom 05.06.2018 – C-210/16 – Wirtschaftsakademie.

77 EuGH, Urteil vom 05.06.2018 – C-210/16 – Wirtschaftsakademie, Rn. 43.

2. Anwendbarkeit der DS-GVO in räumlicher Hinsicht

Eine Besonderheit gegenüber dem alten Datenschutzrecht ist der erweiterte räumliche Anwendungsbereich. Nach Art. 3 Abs. 1 DS-GVO sind alle Verarbeitungsvorgänge im Rahmen einer Niederlassung erfasst. Nach Art. 3 Abs. 2 DS-GVO sind darüber hinaus auch Verarbeitungsvorgänge umfasst, wenn der Verantwortliche zwar nicht in der Union niedergelassen ist, aber Verhalten beobachtet wird, das durch Personen innerhalb der Union stattfindet, oder Waren oder Dienstleistungen Personen in der Union angeboten werden sollen. Im Rahmen von Protokollen bei Haustür-Wahlkämpfen ist die DS-GVO bereits aufgrund der Niederlassung nach Art. 3 Abs. 1 DS-GVO und bei der Erstellung von Profilen zu einzelnen natürlichen Personen – etwa durch Zusammenführung von Daten aus dem Haustürwahlkampf und Marketing-Daten, wie etwa in den USA geschehen – auch nach Art. 3 Abs. 2 lit. b DS-GVO anwendbar.[78] Die Datenverarbeitung durch Facebook, das als verantwortliche Stelle den Sitz in Irland angibt,[79] ist ebenfalls bereits nach Art. 3 Abs. 1 DS-GVO erfasst. Aber selbst Microtargeting für einzelne natürliche Personen mittels Anbieter ohne Niederlassung in der EU ist im Regelfall räumlich nach Art. 3 Abs. 2 lit. b DS-GVO umfasst. Ausreichend ist dafür bereits, dass das beobachtete Verhalten, etwa in Form eines Wählerprofils gespeichert, in der Union erfolgt. Im Hinblick darauf werden die Parteien also auch unter der DS-GVO versuchen, einen Bezug der Daten zu einzelnen Personen vermeiden, um bereits sachlich nicht den Vorgaben der DS-GVO zu unterliegen. Soweit gezielte Online-Werbung über soziale Netzwerke wie Facebook erfolgt, sind jedoch in der Regel sachlicher und räumlicher Anwendungsbereich eröffnet.

In räumlicher Hinsicht sind keine realistischen Microtargeting-Szenarien für innereuropäische Wahlen denkbar, die nicht unter die DS-GVO fielen.

---

78 Vgl. auch Erwägungsgrund 24 (Auszug): „Die Verarbeitung personenbezogener Daten von betroffenen Personen, die sich in der Union befinden, durch einen nicht in der Union niedergelassenen Verantwortlichen oder Auftragsverarbeiter sollte auch dann dieser Verordnung unterliegen, wenn sie dazu dient, das Verhalten dieser betroffenen Personen zu beobachten, soweit ihr Verhalten in der Union erfolgt."

79 https://www.facebook.com/full_data_use_policy (zuletzt abgerufen: 11/2018).

3. Zuständige Datenschutzbehörden unter der DS-GVO

Im datengestützten Haustürwahlkampf, durchgeführt durch Unternehmen mit Sitz in Deutschland, bleiben die deutschen Datenschutzbehörden nach Art. 55 Abs. 1 DS-GVO zuständig.

Im Hinblick auf Microtargeting über soziale Netzwerke wie Facebook bestand unter der Datenschutz-Richtlinie 95/46/EG Uneinigkeit, ob beispielsweise deutsche Behörden eventuelle Verstöße gegen das Datenschutzrecht sanktionieren können.[80] Diese Frage wurde durch den EuGH zugunsten einer weit verstandenen Zuständigkeit der Aufsichtsbehörde beantwortet, sodass bereits unter der Datenschutz-Richtlinie aufgrund der Werbeaktivitäten der deutschen Facebook-Niederlassung auch ein Vorgehen gegen die Facebook Germany GmbH möglich war.[81]

Unter der DS-GVO ist nach dem Grundsatz des Art. 56 Abs. 2 DS-GVO zunächst jede Aufsichtsbehörde räumlich für das Hoheitsgebiet ihres Mitgliedstaates zuständig. Bei grenzüberschreitenden Sachverhalten ist die Aufsichtsbehörde der Hauptniederlassung innerhalb der EU, vgl. Art. 4 Nr. 16 lit. a DS-GVO, federführend zuständig. Im Fall von Facebook wird man hier vermutlich von dem Sitz in Irland ausgehen, soweit nicht Entscheidungen hinsichtlich der Zwecke und Mittel der Datenverarbeitung in Deutschland getroffen werden.

Bisher ist unklar, ob die federführende Zuständigkeit aus Art. 56 Abs. 1 DS-GVO spezieller ist als Art. 55 Abs. 1 DS-GVO[82] oder ob andere nationale Aufsichtsbehörden nach Art. 55 Abs. 1 DS-GVO zuständig bleiben.[83] Für eine Spezialität spricht der Erwägungsgrund 124[84], der nur von

---

80 BVerwG, Beschluss vom 25.02.2016 – 1 C 28.14, ZD 2016, S. 393; OVG Hamburg, Beschluss vom 29.06.2015 – 5 Bs 40/16, NJW 2016, S. 3386.

81 EuGH, Urteil vom 05.06.2018 – C-210/16 – Wirtschaftsakademie, Rn. 64, 74.

82 Kühling/Buchner/Dix, Art. 56 Rn. 6; Hofmann, in: Roßnagel (Hrsg.), Europäische Datenschutz-Grundverordnung, S. 189.

83 Plath/Hullen, Art. 56 Rn. 3; Sydow/Peuker, Art. 56, Rn. 25.

84 Erwägungsgrund 124 (Auszug): „[Die federführende Behörde] sollte mit den anderen Behörden zusammenarbeiten, die betroffen sind, weil der Verantwortliche oder Auftragsverarbeiter eine Niederlassung im Hoheitsgebiet ihres Mitgliedstaats hat, weil die Verarbeitung erhebliche Auswirkungen auf betroffene Personen mit Wohnsitz in ihrem Hoheitsgebiet hat oder weil bei ihnen eine Beschwerde eingelegt wurde."

der Zusammenarbeit mit solchen Behörden spricht, welche die Kriterien aus Art. 56 Abs. 2 DS-GVO erfüllen. Außerdem bräuchte es andernfalls nicht den Begriff der betroffenen Behörde in Art. 4 Nr. 22, Art. 60 DS-GVO. Das „unbeschadet“ in Art. 56 Abs. 1 DS-GVO nimmt nur Bezug auf Art. 55 Abs. 2 und 3 DS-GVO.

Art. 56 Abs. 1 DS-GVO verdrängt somit Art. 55 Abs. 1 DS-GVO. Bei grenzüberschreitenden Sachverhalten ist damit grundsätzlich nach Art. 56 Abs. 1 DS-GVO die Datenschutzbehörde der Hauptniederlassung ausschließlich zuständig – etwa die irische Datenschutzbehörde im Falle von Facebook. Soweit es in der deutschen Sprachversion von Facebook zu möglichen Verstößen kommt oder Beschwerden an deutsche Datenschutzbehörden herangetragen werden, arbeiten diese nach Art. 60, Art. 4 Nr. 22 lit. b bzw. c DS-GVO mit der federführenden Aufsichtsbehörde zusammen. In Streitfragen zwischen diesen Aufsichtsbehörden entscheidet nach Art. 65 Abs. 1 lit. a DS-GVO ein neu eingerichteter europäischer Datenschutzausschuss, vgl. Art. 68 ff. DS-GVO, sodass – anders als bisher – die Einheitlichkeit der Anwendung des Datenschutzrechts auch bei grenzüberschreitenden Sachverhalten sichergestellt wird.

Soweit eine Beschwerde oder ein Verstoß gegen das Datenschutzrecht durch Microtargeting nur Personen eines Mitgliedstaats betrifft bzw. erheblich beeinträchtigt – etwa im Rahmen einer auf Deutschland ausgerichteten Seite wie https://de-de.facebook.com – kann die Datenschutzbehörde dieses Mitgliedstaats nach Art. 56 Abs. 2 und 5 DS-GVO auch ausschließlich zuständig sein. Das setzt die Entscheidung der federführenden Datenschutzbehörde voraus, sich nicht mit dem Fall zu befassen.

Daneben steht die Zuständigkeit für ein Vorgehen gegen die werbenden Parteien als (Mit-)Verantwortliche.

Unabhängig von der Zuständigkeit einer Datenschutzbehörde kann sich nach Art. 77 Abs. 1 DS-GVO eine betroffene Person an die Datenschutzbehörde seines Mitgliedstaats wenden.

4. Datenschutzgrundsätze unter der DS-GVO

Warum es für deutsche Parteien so entscheidend ist, den Personenbezug der Daten zu verhindern und welche Konsequenzen sich für das

Microtargeting über soziale Netzwerke ergeben, zeigt ein Blick auf die Datenschutzgrundsätze und die Erlaubnistatbestände unter der DS-GVO.

Das „Ob“ der Verarbeitung richtet sich maßgeblich nach Art. 6 DS-GVO und der Frage, ob einer der dort normierten Erlaubnistatbestände greift. Einer dieser Erlaubnistatbestände ist nach Art. 6 Abs. 1 lit. a DS-GVO die Einwilligung der betroffenen Person. Für den Haustürwahlkampf wäre so etwa die Einwilligung praktikabel. Dabei sind die Freiwilligkeit, vgl. Art. 7 Abs. 4 DS-GVO,[85] und die jederzeitige Widerruflichkeit für die Zukunft nach Art. 7 Abs. 3 DS-GVO zu beachten. In der Praxis des Microtargetings, etwa im Haustürwahlkampf, bleibt zweifelhaft, wie viele Nutzer eine derartige Einwilligung erteilen würden, um den Parteien einen effizienteren Wahlkampf zu ermöglichen.

Soweit man in Wahlwerbezwecken ein berechtigtes Interesse[86] der Parteien und der sozialen Netzwerke sieht, ist dies nach Art. 6 Abs. 1 lit. f DS-GVO jedoch bereits ausreichend, wenn nicht die Interessen des Betroffenen überwiegen.[87] Zumindest im Hinblick auf die Parteien und unmittelbare Wahlwerbung durch diese, kann der verfassungsmäßige Auftrag der Parteien zur Mitwirkung an der Willensbildung, vgl. Art. 21 Abs. 1 S. 1 GG, als berechtigtes Interesse angesehen werden. Allerdings reicht dieser Erlaubnistatbestand für umfangreiche Profile einzelner Wähler nicht aus, da diese nicht mehr erforderlich wären.[88]

Die Verarbeitung ist nach Art. 5 Abs. 1 lit. b, c DS-GVO an den ursprünglich festgelegten Zweck gebunden und die Verarbeitung darf nur erfolgen,

---

85 Siehe auch Erwägungsgrund 32 (Auszug): „Die Einwilligung sollte durch eine eindeutige bestätigende Handlung erfolgen, […] freiwillig, für den konkreten Fall, in informierter Weise und unmissverständlich“ und Erwägungsgrund 43 (Auszug): „Die Einwilligung gilt nicht als freiwillig erteilt, […] wenn die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung abhängig ist, obwohl diese Einwilligung für die Erfüllung nicht erforderlich ist.“

86 Vgl. umfangreich zur Auslegung dieses Erlaubnistatbestands das Dossier „Ich sammele, also bin ich (Social Credit) – Das Szenario eines allumfassenden Bonitätssystems am Beispiel Chinas“ (G.).

87 Zumindest Direktwerbung kann ein berechtigtes Interesse sein, vgl. Erwägungsgrund 47 (Auszug): „Die Verarbeitung personenbezogener Daten zum Zwecke der Direktwerbung kann als eine einem berechtigten Interesse dienende Verarbeitung betrachtet werden.“

88 Richter, DÖV 2013, S. 961, 963.

soweit es für die Zwecke notwendig ist. Zur Ermittlung der Reichweite des Zwecks bietet die Auslegungsregel[89] des Art. 6 Abs. 4 DS-GVO Anhaltspunkte. Gerade soziale Netzwerke setzen große Datenmengen voraus. Soweit aber aus Profil-Angaben, den Interessen von Freunden oder den eigenen „Klicks“ neue Erkenntnisse gewonnen werden, lässt sich daran zweifeln, ob diese noch notwendig sind.[90] Eine nachträgliche Weitergabe von Daten, etwa durch Anbieter wie Payback, an Parteien wäre daran zu messen.

Die Identifizierung der Personen darf nur solange möglich sein, solange es für die Verarbeitungszwecke erforderlich ist, Art. 5 Abs. 1 lit. b, c, e DS-GVO. Microtargeting durch den Ankauf von Marketing-Daten, wie in den USA, steht dabei insbesondere der Zweckbindungsgrundsatz nach Art. 5 Abs. 1 lit. b DS-GVO entgegen. Dieser spielt aus diesem Grund regelmäßig bei dem Einsatz von Big-Data-Technologien eine Rolle.[91] Verstöße gegen die in Art. 5 Abs. 1 DS-GVO genannten Grundsätze können selbstständig sanktioniert werden, auch wenn durch einen Verstoß nicht notwendigerweise die eigentliche Verarbeitung als rechtswidrig anzusehen ist.[92] Gerade im Hinblick auf soziale Netzwerke wird sich zeigen, wie eng Grundsätze der Zweckbindung, Datenminimierung und Speicherbegrenzung in der Rechtsanwendung ausgelegt werden und inwieweit so gegebenenfalls das Microtargeting über soziale Netzwerke eingeschränkt wird.

In Ansehung des Zwecks sind etwa bei sozialen Netzwerken, die gerade massenhaft Daten erfordern, weitergehende – aber ebenfalls nicht grenzenlose – Datensammlungen denkbar.[93]

Im Rahmen des Microtargetings sind in der Regel Daten betroffen, aus denen die politische Meinung hervorgehen kann, Art. 9 Abs. 1 DS-GVO.

---

89 Kühling/Buchner/Petri, Art. 6, Rn. 183.

90 Nebel, Facebook knows your vote! – Big Data und der Schutz politischer Meinung in sozialen Netzwerken, in: Richter (Hrsg.), Privatheit, Öffentlichkeit und demokratische Willensbildung in Zeiten von Big Data, S. 105.

91 Culik/Döpke, Zweckbindungsgrundsatz gegen unkontrollierten Einsatz von Big Data-Anwendungen, ZD 2017, 226.

92 Herbst, in: Kühling/Buchner (Hrsg.), Datenschutz-Grundverordnung, Art. 5 Rn. 2.

93 Nebel, S. 105.

Diese bedürfen zusätzlich[94] eines besonderen Erlaubnistatbestands (Art. 9 Abs. 2 DS-GVO, §§ 22, 27 f. BDSG 2018). Soweit Nutzer sozialer Netzwerke ihre Einstellung z. B. durch den Like einer Partei-Seite selbst in dem gesamten, öffentlich zugänglichen Netzwerk[95] kundtun, sind sie nicht schutzwürdig und Art. 9 Abs. 2 lit. e DS-GVO greift. Wird der mutmaßliche politische Wille aufgrund von Korrelationen, etwa aus einem Freundeskreis mit vielen Likes zu Gunsten einer Partei, ermittelt, greift der Erlaubnistatbestand nicht mehr. In letzterem Fall kommt regelmäßig nur eine Einwilligung nach Art. 9 Abs. 2 lit. a DS-GVO in Betracht. Diese wiederum muss zumindest den nicht zu unterschätzenden Anforderungen aus Art. 7 DS-GVO im Hinblick auf vorherige Aufklärung und Freiwilligkeit genügen.

VII. Fazit

Microtargeting mit all seinen Möglichkeiten ist längst in den US-Wahlkämpfen angekommen. In Deutschland wagt man ebenfalls erste Versuche in der gezielten Wähleransprache – sei es über soziale Netzwerke oder im datengestützten Haustürwahlkampf. Das deutsche bzw. europäische Datenschutzrecht setzt allerdings enge Grenzen, sodass im Wahlkampf besonders darauf geachtet wird, einen Personenbezug zu vermeiden, um gerade nicht den Restriktionen des Datenschutzrechts zu unterliegen.

Die tatsächliche Bedeutung des praktizierten Microtargetings lässt sich kaum sicher ermitteln aufgrund der zahlreichen Faktoren, die Einfluss auf ein erfolgreiches Wahlergebnis haben. Daher bleibt den Parteien nichts anderes übrig als entweder den Verheißungen von mehr Effizienz im Wahlkampf zu vertrauen oder Nachteile wie einen drohenden „Wahlkampf im Untergrund“ stärker zu gewichten. Microtargeting besitzt das Potential, den Wettbewerb der Meinungen zu beeinflussen. Kommende Wahlkämpfe werden zeigen, inwieweit sich deutsche und europäische

---

94 Vgl. auch Erwägungsgrund 51: „[…] Zusätzlich zu den speziellen Anforderungen an eine derartige Verarbeitung [besonderer Kategorien personenbezogener Daten] sollten die allgemeinen Grundsätze […], insbesondere hinsichtlich der Bedingungen für eine rechtmäßige Verarbeitung, gelten […]“.

95 Nebel, S. 103.

Parteien unter der DS-GVO an das Microtargeting weiter herantasten und welche Auswirkungen die eigene Verantwortlichkeit der Werbenden auf die Nutzung von sozialen Netzwerken wie Facebook im Wahlkampf hat.

Literaturnachweise

Agan, Silent Marketing: Microtargeting, http://www.wpp.com/wpp/marketing/reportsstudies/silentmarketing/ (zuletzt abgerufen: 11/2018).

Barocas, The Price of Precision: Voter Microtargeting and Its Potential Harms to the Democratic Process, in: Proceedings of the first edition workshop on Politics, elections and data 2012, S. 31 ff.

Confessore/Hakim, Data firm says 'secret sauce' aided Trump; many scoff, https://www.nytimes.com/2017/03/06/us/politics/cambridge-analytica.html (zuletzt abgerufen: 11/2018).

Culik/Döpke, Zweckbindungsgrundsatz gegen unkontrollierten Einsatz von Big Data-Anwendungen, ZD 2017, S. 226-230.

Edsall, Let the Nanotargeting begin, https://campaignstops.blogs.nytimes.com/2012/04/15/let-the-nanotargeting-begin/ (zuletzt abgerufen: 11/2018).

Heinrich Böll Stiftung, Microtargeting – digitales Marketing, https://www.boell.de/de/2017/02/09/microtargeting-digitales-marketing (zuletzt abgerufen: 11/2018).

Jungherr, Datengestützte Verfahren im Wahlkampf, http://andreasjungherr.net/wp-content/uploads/2017/03/Jungherr-2017-Datengest%C3%BCtzte-Verfahren-im-Wahlkampf-Preprint.pdf (zuletzt abgerufen: 11/2018).

Jungherr/Schoen, Das Internet in Wahlkämpfen – Handreichung zur politischen Bildung – Band 12, http://www.kas.de/wf/doc/kas_34855-544-1-30.pdf (zuletzt abgerufen: 11/2018).

Kühling/Buchner, Datenschutz-Grundverordnung, 2. Auflage München 2018.

Nebel, Facebook knows your vote! – Big Data und der Schutz politischer Meinung in sozialen Netzwerken, in: Richter (Hrsg.), Privatheit, Öffentlichkeit und demokratische Willensbildung in Zeiten von Big Data, S. 89-110, Baden-Baden 2015.

Papakyriakopoulos/Shahrezaye/Thieltges/Medina Serrano/Hegelich, Social Media und Microtargeting in Deutschland, Informatik-Spektrum 2017, S. 327-335.

Plath, BDSG/DSGVO, 2. Auflage Köln 2016.

Richter, Die Wahl ist geheim… so what?, DÖV 2013, S. 961-970.

Roßnagel, Europäische Datenschutz-Grundverordnung, 1. Auflage Baden-Baden 2017.

Sydow, Europäische Datenschutzgrundverordnung, 1. Auflage Baden-Baden 2017.

Zuiderveen Borgesius et al., Online Political Microtargeting: Promises and Threats for Democracy, Utrecht Law Review 2018 (14), S. 82-96.

F. Big Social Data (Tristan Julian Tillmann)

Stand: Januar 2018

Abstract: Big Social Data

Immer mehr Menschen nutzen soziale Netzwerke. Das bekannteste und meist genutzte ist Facebook. Facebook hat aktuell mehr als zwei Milliarden Nutzer, die jeden Tag unzählige Daten produzieren. Neueste Studien zeigen, welche Informationen sich durch Big-Data-Anwendungen aus diesen Daten generieren lassen. Dies birgt ein nicht zu unterschätzendes Risiko für jeden einzelnen Nutzer. Es entstehen jedoch auch vielfältige Möglichkeiten für Firmen und staatliche Stellen, adäquater und schneller auf Veränderungen und andere Anforderungen der Bevölkerung zu reagieren. Der vorliegende Beitrag zeigt auf, welchen tatsächlichen Informationsgehalt Facebook-Profile enthalten.

I. Einleitung

„Liberae sunt […] nostrae cogitationes."

Cicero, Rede für Milo, XXIX, 79.

Unsere Gedanken sind frei. Dem überwiegenden Teil der deutschen Bevölkerung kommt bei diesem Leitmotiv ein bekanntes deutsches Volkslied[1] in den Sinn. Zuletzt sang Jan Böhmermann dieses bei einer Solidaritätslesung zugunsten des in der Türkei inhaftierten Journalisten Deniz Yücel im Schauspiel Frankfurt.[2] Der Gedanke dahinter taucht in der Geschichte jedoch häufiger auf. Schon Marcus Tullius Cicero hielt im Jahr

---

1 Breuer, S. 118.

2 http://www.hessenschau.de/kultur/jan-boehmermann-singt-in-frankfurt-fuer-inhaftierten-journalisten-yuecel,freedeniz-lesung-schauspielfrankfurt-100.html (zuletzt abgerufen: 11/2018).

52 v. Chr. eine Apologie für den des Mordes angeklagten Titus Annius Milo, in der er das obige Zitat ausspricht. Der Wert dieser Aussage war und ist den freien, denkenden Menschen seit jeher bewusst. Es ist ein nicht zu unterschätzendes, hohes Gut.

Mit der stattfindenden Digitalisierung und dem verstärkten Einfluss von Big Data stellt sich die Frage, ob dieser Glaube an die Freiheit der Gedanken noch Gültigkeit hat. Auf den ersten Blick mag es frevelhaft erscheinen, eine solche fundamentale Säule einer freien Gesellschaft anzutasten. Denn der Bevölkerung ist es mittlerweile durchaus bewusst, dass den Betreibern von sozialen Netzwerken und anderen Plattformen bis hin zu zukünftigen Arbeitgebern eine Menge Daten, zum Teil auch persönlichster Art, bekannt sein können. Insbesondere jüngere Menschen „teilen“ online eine Vielzahl von persönlichen Informationen. Neueste Studien zeigen, dass auf Big Data gestützte Techniken verblüffende Möglichkeiten bieten. Bei diesen geht es nicht um die Sammlung von freiwillig öffentlich oder „privat“ geteilten Informationen, sondern um die Generierung völlig neuer Daten. So können unter Umständen Informationen ermittelt werden, denen sich der Einzelne über seine eigene Persönlichkeit überhaupt nicht bewusst ist oder die er mit absolut niemandem zu teilen bereit ist. So beginnt ein Szenario, welches sich für die wohl meisten Bürger der freien Welt als dystopisch darstellt.

Gerade Facebook stellt ein Paradebeispiel für einen riesigen Datensammler dar. Über jeden Nutzer und auch über Nicht-Nutzer sind eine Fülle von Informationen hinterlegt. Längst werden Bekanntschaften aus dem realen Leben „gestalked“, um vermeintlich zu wissen, mit wem man es zu tun hat. Wissenschaftler hingegen sehen in Facebook eine Ansammlung von Probanden, deren Daten für sozialwissenschaftliche und psychologische Studien verwendet werden können. Ein Grund dafür ist, neben den verästelten sozialen und semantischen Daten, dass diese ohne allzu großen Aufwand ausgelesen werden können.[3]

---

3 Lambiotte/Kosinski, S. 1934, 1935.

II. Social Data vor dem Einsatz von Big-Data-Technologien

Der Umfang an verfügbaren Daten über jeden einzelnen Internetnutzer ist schon seit langem enorm. Insbesondere Nutzer von sozialen Netzwerken wie Facebook, Instagram & Co. sind für die dahinterstehenden Firmen mehr oder weniger gläsern. Aber auch, wer sich von sozialen Netzwerken fernhält, hinterlässt eine deutliche Spur, die beispielsweise von Webtrackern[4] oder direkt beim Internetdienstanbieter aufgezeichnet wird. Des Weiteren werden „offline"-Aktivitäten, beispielweise durch das Smartphone (z.B. durch Location-based Services)[5] oder durch eine Vielzahl von anderen Möglichkeiten digital registriert und überwacht.[6] Ein Auslesen und Analysieren der so gesammelten Daten ist mitunter sehr einfach und wird auch praktiziert. Es scheint ein vollumfänglich privates Leben im 21. Jahrhundert nicht mehr zu geben.[7]

Bisher ist es so, dass diese Daten lediglich eine Sammlung von Informationen aus der Vergangenheit und Gegenwart darstellen. Das so entstehende Bild ist kongruent mit dem Wissen der Person über sich selbst.[8] Auch bei Zugrundelegung dieser Prämisse gilt es, vorsichtig mit persönlichen Daten umzugehen. Denn die gesammelten und von Internetnutzern öffentlich bereitgestellten Daten erlauben es, Individuen online zu durchleuchten. Es entstehen umfassende Nutzerprofile, die vom Einzelnen nicht mehr kontrolliert und überblickt werden können.[9] Privatpersonen und Unternehmen nutzen diese in großem Umfang zum Beispiel zur Optimierung ihres Angebots oder um gezielt Werbung zu adressieren. Dennoch bewerten insbesondere jüngere Teile der Bevölkerung das bestehende Risiko anders als es Nicht-„Digital Native"-Generationen tun.

---

4 Röttgen, in: Hoeren/Kolany-Raiser (Hrsg.), Big Data zwischen Kausalität und Korrelation, S. 84-94.

5 Pieringer, Journal of Law, Technology & Policy 2012, S. 559, 563.

6 Kosinski/Stillwell/Graepel, PNAS 2013, S. 5802; Lambiotte/Kosinski, S. 1934, 1937.

7 Solberg, Journal of Law, Technology & Policy 2010, S. 311, 327; http://nymag.com/news/features/27341/index2.html (zuletzt abgerufen: 11/2018).

8 Hermstrüwer, S. 94.

9 Dienlin, S. 118.

Vor allem auf Social-Media-Plattformen stellen sie sich, zum Teil hemmungslos, dar.[10]

III. Big-Data-unterstützte Generierung von Informationen

Big-Data-Technologien ermöglichen nun ganz neue Wege. Big Data umfasst eine Datenansammlung, die so groß, komplex, schnell und schwach strukturiert ist, dass sie mit normalen Datenbankmethoden nicht mehr verarbeitet werden kann.[11] Diese Datenmassen können verschiedenen Analyse-Algorithmen ausgesetzt werden, um Muster und Zusammenhänge zu ermitteln.[12] Es geht somit nicht nur um das bloße Abrufen von gesammelten Informationen[13], sondern um das Generieren von neuen Daten. Google soll durch Beobachtung des Suchverhaltens zum Beispiel in der Lage sein, den Beginn einer Grippewelle bestimmen zu können.[14] Den einzelnen Nutzer betreffend können Informationen ermittelt werden, die dieser womöglich selbst nicht kennt oder die er bisher niemals mit einem anderen Menschen geteilt hat.[15] Es besteht sogar die Möglichkeit, Entscheidungen von Personen und Personengruppen vorherzusagen.[16]

1. „Schattenprofile“

Über die vom User in sein Profil eingepflegten Daten hinaus erstellt Facebook ein sogenanntes „Schattenprofil“. Dieses speist sich aus einer Vielzahl von Informationen, die der Betroffene dem sozialen Netzwerk nie bereitgestellt hat. Jedes Mal, wenn die Kontaktdaten eines Smartphones

---

10 http://nymag.com/news/features/27341/index2.html (zuletzt abgerufen: 11/2018).

11 Roßnagel, ZD 2013, S. 562; Simo, S. 14.

12 Roßnagel, ZD 2013, S. 562; Hermstrüwer, S. 94/95; Wolf, S. 25.

13 Hermstrüwer, S. 94.

14 Weichert, ZD 2013, S. 251, 254; http://www.spiegel.de/lebenundlernen/job/student-der-tu-darmstadt-will-mit-computer-die-zukunft-voraussagen-a-938593.html (zuletzt abgerufen: 11/2018).

15 Hermstrüwer, S. 94/95/366.

16 Hermstrüwer, S. 94/95; Nebel, S. 89; Roßnagel, ZD 2013, S. 562.

Facebook zur Verfügung gestellt werden, versucht Facebook Querverbindungen zu finden.[17] Tun dies auch nur wenige „Freunde“, hat Facebook Zugriff auf eine Unmenge von Informationen, die der einzelne User Facebook gegebenenfalls nicht überlassen wollte (z.B. verschiedene E-Mail-Adressen, Kontaktfotos, Handynummer(n)). Somit kennt Facebook wahrscheinlich jede Adresse, an der ein bestimmter User jemals gelebt hat, jede E-Mail-Adresse und Telefonnummer, die er jemals besessen hat und vieles mehr.[18] Diese „Schattenprofile“ erlauben es Facebook, die sozialen Interaktionen genauestens zu verfolgen. Facebook kann darüber hinaus jedoch auch ermitteln, welche Personen sich wahrscheinlich kennen und diesen „Freunde“ vorschlagen. Besonders brisant wird dies, wenn Facebook einem User, der eine vermeintlich anonyme Samenspende abgegeben hat, Jahre später seine biologische Tochter als „Freund“ vorschlägt.[19]

2. Profilbildanalyse

Täglich laden die User des populärsten[20] sozialen Netzwerks Facebook eine Vielzahl von Bildern hoch. Das „wichtigste“ ist natürlich das Profilbild. Ist der User auf diesem Profilbild zu sehen, kann es mit Hilfe eines Algorithmus analysiert werden. Mit Hilfe von Künstlichen Neuronalen Netzwerken werden riesige Datenmengen, wie zum Beispiel Bilddateien, analysiert und so Muster ermittelt.[21] Diese übertreffen schon heute menschliche Fähigkeiten, beispielsweise bei der Erkennung von Hautkrebs.[22] Einer neuesten Studie zufolge ist es jedoch auch möglich, die sexuelle Orientierung des Users zu ermitteln. Dabei wurde zunächst ein Künstliches

---

17 https://gizmodo.com/how-facebook-figures-out-everyone-youve-ever-met-18198 22691 (zuletzt abgerufen: 11/2018).

18 https://gizmodo.com/how-facebook-figures-out-everyone-youve-ever-met-18198 22691 (zuletzt abgerufen: 11/2018).

19 https://gizmodo.com/how-facebook-figures-out-everyone-youve-ever-met-18198 22691 (zuletzt abgerufen: 11/2018).

20 https://techcrunch.com/2017/06/27/facebook-2-billion-users/ (zuletzt abgerufen: 11/2018).

21 Kosinski/Wang, S. 5.

22 Esteva et al., S. 115, 117.

Neuronales Netzwerk mit Bildern von hetero- und homosexuellen Menschen trainiert, damit es Muster ermitteln konnte. Sodann wurden diesem zwei Bilder vorgelegt, bei denen es zu entscheiden hatte, welche Person hetero- und welche homosexuell ist.[23] Die Erfolgsquote lag, bezogen auf Facebook-Bilder, bei 74 Prozent.[24] Im Gegensatz dazu liegen menschliche Einschätzungen lediglich bei einer Trefferquote zwischen 55 und 65 Prozent.[25] Die Risiken, die hinter dieser Technik stecken, sind nicht zu unterschätzen. Der digitale Fußabdruck, den die Nutzer von sozialen Netzwerken hinterlassen, kann zwar minimiert werden, aber das eigene Gesicht lässt sich nicht einfach verändern. Auf Grund der Omnipräsenz von Smartphones lassen sich von Personen ohne große Hindernisse Bilder erstellen und ggf. analysieren. Besondere Brisanz besteht in Ländern, in denen Homosexualität nicht nur verboten, sondern teilweise sogar mit der Todesstrafe bedroht wird.[26]

3. Aussagekraft von „Likes“ und der Sprache

Auf Facebook teilen die User eine Vielzahl von mitunter sensiblen Daten. Facebook erlaubt den Usern aber vor allem mit Hilfe eines „Likes“ ihre Zustimmung einfach und vermeintlich risikolos auszudrücken. Tatsächlich zeigen Studien, dass diese „Likes“ mit Hilfe von Big-Data-Technologien enormes Aussagepotential enthalten. Wissenschaftler sind in der Lage einige hoch sensible Eigenschaften der User zu bestimmen. Dazu gehören die sexuelle Orientierung, die Ethnie, die religiösen und politischen Ansichten, Alter, Geschlecht, Charakterzüge, Zufriedenheit und ob die Eltern getrennt leben.[27] Diese Bestimmung erfolgt automatisiert und mit einer hohen Treffsicherheit. Nur über die „Likes“ ist es mit einer Wahrscheinlichkeit von 93 Prozent möglich das Geschlecht, von 85 Prozent die politische Ansicht („Democrat“ oder „Republican“) und von 88 Prozent

---

23 Kosinski/Wang, S. 16.

24 Kosinski/Wang, S. 29.

25 Rule/Ambady/Hallett, S. 1245, 1246/1247; Kosinski/Wang, S. 27.

26 https://www.washingtonpost.com/news/worldviews/wp/2016/06/13/here-are-the-10-countries-where-homosexuality-may-be-punished-by-death (zuletzt abgerufen: 11/2018).

27 Kosinski/Stillwell/Graepel, PNAS 2013, S. 5802.

zu bestimmen, ob ein männlicher User homosexuell ist.[28] Die Wissenschaftler haben Verbindungen zwischen der zu bestimmenden Eigenschaft und dem „gelikedten“ Inhalt erstellt. So ist zum Beispiel ein guter Indikator für hohe Intelligenz das „liken“ von Seiten wie „Science“ oder „Thunderstorms“, wohingegen eine geringe Intelligenz mit „Harley Davidson“ oder „I Love Being A Mom“ korreliert. Besonders brisant ist, dass zum Teil bereits ein einziger „Like“ ausreicht, um eine nicht zu vernachlässigende Aussage zu treffen. Wenn man bedenkt, dass der gemeine User deutlich mehr „Likes“ verteilt, steigt die Aussagefähigkeit erheblich an.[29] Zudem ist zu berücksichtigen, dass statt „Likes“ auch andere digitale Aufzeichnungen in dieser Weise verwendet werden können. Beispielhaft sind der Browser-Verlauf und Sucheinträge bei Suchmaschinen zu nennen.[30]

Nimmt man nun noch das klassische Hilfsmittel des Big-Five-Modells (auch OCEAN-Modell) zur Hand, lassen sich aus den Facebook-„Likes“ noch weitere Informationen erlangen. Das Big-Five-Modell ist international als Standardmodell der Persönlichkeitserforschung anerkannt.[31] Demnach bestehen fünf Hauptdimensionen der Persönlichkeit: Offenheit, Gewissenhaftigkeit, Extraversion, Verträglichkeit und Neurotizismus.[32] Je nachdem wie ausgeprägt die einzelnen Faktoren sind, lassen sich Aussagen über die Persönlichkeit eines Menschen machen. Diese können dazu verwendet werden, um zu bestimmen, wie sich ein Mensch tendenziell verhalten wird. Beispielsweise konnte ein Zusammenhang zwischen Extraversion und dem unentschuldigten Fernbleiben von Arbeitnehmern nachgewiesen werden.[33]

Die Wissenschaft ist durch die Kombination von „Likes“ und dem Big-Five-Modell in der Lage, zu bestimmen wie eine Testperson bestimmte

---

28 Kosinski/Stillwell/Graepel, PNAS 2013, S. 5802, 5803.

29 Kosinski/Stillwell/Graepel, PNAS 2013, S. 5802, 5804.

30 Kosinski/Stillwell/Graepel, PNAS 2013, S. 5802, 5805.

31 Lambiotte/Kosinski, S. 1934; De Raad/Perugini, S. 3/5.

32 Collins et al., S. 25; De Raad/Perugini, S. 6.

33 De Raad/Perugini, S. 6.

Fragen beantworten wird.[34] Eine Computer-gestützte Persönlichkeitseinschätzung, die auf Facebook-„Likes“ basiert, ist in der Lage, sogar die Selbsteinschätzung des Users zu übertreffen.[35] Es werden lediglich 10, 70, 150 bzw. 300 „Likes“ benötigt, um einen durchschnittlichen Arbeitskollegen, einen Freund, ein Familienmitglied und den Partner in den Schatten zu stellen.[36] Die zugrunde liegenden Studien zeigen, dass soziale Netzwerke einen ausreichenden Umfang an Informationen enthalten, um akkurat die Persönlichkeit eines Menschen zu bestimmen.[37] Die Universität Cambridge betreibt eine Web-Anwendung, die die Persönlichkeit bestimmt. Die Anwendung analysiert, je nachdem welcher digitale Fingerabdruck zur Verfügung gestellt wird, die Facebook „Likes“ oder Twitter Posts.[38] Eine Anwendung, die ebenso verführerisch wie angsteinflößend ist.

Doch Facebook enthält neben den „Likes“ einige weitere Informationsquellen.[39] Ebenfalls mit Hilfe des Big-Five-Modells konnten Wissenschaftler die allgemeine Zufriedenheit mit dem Leben der User sicher bestimmen. Dazu verwendeten sie neben den „Likes“ auch die Anzahl an „Freunden“, die Anzahl von „Tags“ auf Fotos, das Alter, den Beziehungsstatus und die in Posts verwendeten Wörter.[40] Gerade letztere bieten eine große Angriffsfläche. Persönliche Charakteristiken werden auch durch unsere Sprache, das heißt durch verwendete Wörter und Stilistik, ausgedrückt.[41] Eine Analyse von Facebook Posts von mehr als 69.000 Facebook Usern hat ergeben, dass zum Beispiel „fucking“ oder „sick_of“ auf eine niedrige emotionale Stabilität hinweist und „lakersbasketball“ und

---

34 https://www.dasmagazin.ch/2016/12/03/ich-habe-nur-gezeigt-dass-es-die-bombe-gibt/ (zuletzt abgerufen: 11/2018).

35 Youyou/Kosinski/Stillwell, PNAS 2015, S. 1036.

36 Youyou/Kosinski/Stillwell, PNAS 2015, S. 1036, 1037.

37 Kern et al, S. 158, 166.

38 https://applymagicsauce.com/ (zuletzt abgerufen: 11/2018).

39 Lambiotte/Kosinski, S. 1934, 1935.

40 Collins et al., S. 31.

41 Kern et al., S. 158.

„beach“ eher auf eine hohe.[42] Jeder Post bei Facebook hinterlässt eine Spur zur eigenen Persönlichkeit.[43]

Aus diesem Wissen kann Macht generiert werden. Gerade Firmen dürften an diesen Möglichkeiten größtes Interesse haben. Zunächst könnte beispielweise ermittelt werden, welche Bedürfnisse entstehen werden.[44] Kunden und mögliche Neukunden könnten einem „Targeting“ ausgesetzt werden, womöglich bevor diese selbst wissen, dass ein Bedürfnis nach dem angebotenen Produkt besteht.[45] Maßgeschneiderte Nachrichten, die automatisch, genau und, da personalarm, kostengünstig versendet werden, sind keine Zukunftsmusik mehr. Zudem kann allgemein das Kundenverhalten studiert werden, um strategische Entscheidungen besser treffen zu können.[46] Ein psychologisches Targeting, bei dem lediglich ein einziger „Like“ zur Bestimmung des psychologischen Profils zugrunde gelegt wird, kann die Clickraten von Facebook-Anzeigen um über 60 Prozent steigern.[47] Wenn man die Möglichkeiten bedenkt, die entstehen, wenn man ein vollständiges psychologisches Profil zu Grunde legt, kann einem angst und bange werden. Diese Technik könnte dazu verwendet werden, um Schwächen auszunutzen und z. B. direkt Glücksspiel- oder Alkoholwerbung an entsprechend anfällige Personen zu adressieren.[48] Auch Human-Resource-Abteilungen könnten zukünftige Arbeitnehmer vollumfänglich auf eine Kompatibilität mit dem Job und der Firma überprüfen.[49] Diese Modelle und Methoden bringen die Gefahr der Beeinflussung und Manipulation mit sich.

---

42 Kern et al., S. 158, 162.

43 Kern et al., S. 158, 166.

44 BITKOM, S. 36/37; https://www.forbes.com/sites/louiscolumbus/2016/05/09/ten-ways-big-data-is-revolutionizing-marketing-and-sales/#4f4873c121cf (zuletzt abgerufen: 11/2018).

45 Lambiotte/Kosinski, S. 1934.

46 Stoicescu, Database Systems Journal 2015, S. 28, 29.

47 Matz et al., S. 3.

48 Matz et al., S. 4.

49 Youyou/Kosinski/Stillwell, PNAS 2015, S. 1036, 1039.

IV. Fazit

Die „Freiheit der Gedanken“ ist nicht vollständig in Gefahr. Allerdings gibt es im Zeitalter von Big Data die Möglichkeit, schnell und automatisiert viele Informationen über einzelne Personen zu erlangen. Und wie gezeigt geht die Analyse schon viel weiter. Die psychologischen Eigenschaften und Einstellungen können analysiert und bewertet werden, ohne dass der Einzelne etwas davon mitbekommt.[50] So besteht durchaus die Möglichkeit, dass in Zukunft beispielsweise Human-Resource-Abteilungen auf solche und ähnliche Techniken zurückgreifen, um zukünftige Mitarbeiter zu screenen. Anders als bisher könnte es nicht nur um ein Sammeln von „status quo“-Informationen gehen, also solchen, die der Einzelne „freiwillig“ zum Beispiel über soziale Netzwerke preisgegeben hat. Möglich könnten Prognosen über Entwicklungspotentiale und zusätzliche Informationen sein, die der Betroffene gar nicht preiszugeben bereit ist und unter Umständen bisher niemals preisgegeben hat. So kann die Gefahr von Diskriminierungen und Entscheidungen, die auf nicht richtigen Fakten beruhen, entstehen.[51] Denn Big-Data-Anwendungen sind nicht unfehlbar.

Die neuen Möglichkeiten stellen einen enormen Verlust an Privatsphäre dar. Die User können nicht überblicken, welche preisgegebene Information zu welchem Wissensstand führt und wer diesen generiert bzw. nutzt. Die Rekombination- und Aggregationsmöglichkeiten mit anderen Daten sind unendlich und mit den Informationen wird auch in Zukunft immer weiter gearbeitet. Eine informierte Einwilligung in die Sammlung und Verarbeitung von Daten ist vor diesem Hintergrund schlicht nicht möglich. Jeder einzelne muss sich nicht nur fragen, ob er diese konkrete Information öffentlich machen möchte, sondern auch, welche Kreuzverbindungen möglichweise entstehen können. Diese letzte Frage lässt sich im Grunde nicht beantworten, da die in den Studien eingesetzten Verfahren und Algorithmen viel zu komplex sind. Im Grunde kann demjenigen, der seine Daten nicht zum Nulltarif unters Volk bringen will, nur angeraten

---

50 Lambiotte/Kosinski, S. 1934, 1938.

51 Hermstrüwer, S. 97; Nebel, S. 97.

werden, so wenig Daten wie möglich öffentlich zu machen. Ob dies im 21. Jahrhundert ein realistischer Rat ist, sei dahingestellt.

Literaturnachweise

BITKOM, Big Data im Praxiseinsatz – Szenarien, Beispiele, Effekte, Berlin 2012.

Breuer, Der Zupfgeigenhansl, 90. Auflage Leipzig 1920.

Cicero, Rede für Milo, hrsg. u. übers. v. Giebel, Stuttgart 1986.

Collins et al., Are You Satisfied with Life?: Predicting Satisfaction with Life from Facebook, in: Agarwal/Xu/Osgood (eds), Social Computing, Behavioral-Cultural Modeling, and Prediction 2015.

De Raad/Perugini, Big Five Assessment, Seattle 2002.

Dienlin, Ist die politische Meinung privat oder öffentlich? Der Blick der Medienpsychologie, in: Roßnagel (Hrsg.), Privatheit, Öffentlichkeit und demokratische Willensbildung in Zeiten von Big Data, Baden-Baden 2015.

Esteva et al., Dermatologist – level classification of skin cancer with deep neural networks, Nature 2017, S. 115-118.

Hermstrüwer, Informationelle Selbstgefährdung, Tübingen 2016.

Kern et al., The Online Social Self: An Open Vocabulary Approach to Personality, Assessment 2014, S. 158-169.

Kosinski/Stillwell/Graepel, Private traits and attributes are predictable from digital records of human behavior, PNAS 2013, S. 5802-5805.

Kosinski/Wang, Deep neural networks can detect sexual orientation from faces, wird erscheinen in: Journal of Personality and Social Psychology, aktuelle Version abrufbar unter: https://osf.io//zn79k/ (zuletzt abgerufen: 11/2018).

Kosinski et al., Mining Big Data to Extract Patterns and Predict Real-Life Outcomes, Psychological Methods 2016, S. 493-506.

Lambiotte/Kosinski, Tracking the Digital Footprints of Personality, Proceedings of the IEEE 2014, S. 1934-1939.

Matz et al., Psychological targeting as an effective approach to digital mass persuasion, PNAS Early Print, http://www.pnas.org/content/early/2017/11/07/1710966114.full (zuletzt abgerufen: 11/2018).

Nebel, Facebook knows your vote! – Big Data und der Schutz politischer Meinung in sozialen Netzwerken, in: Roßnagel (Hrsg.), Privatheit, Öffentlichkeit und demokratische Willensbildung in Zeiten von Big Data, Baden-Baden 2015.

Pieringer, There's No App For That: Protecting Users From Mobile Service Providers And Developers Of Location-Based Applications, Journal of Law, Technology & Policy 2012, S. 559-577.

Röttgen, Gefällt mir, gefällt mir nicht – Tracking im Internet, in: Hoeren/Kolany-Raiser (Hrsg.), Big Data zwischen Kausalität und Korrelation, S. 84-94, Münster 2016.

Roßnagel, Big Data – Small Privacy? Konzeptionelle Herausforderungen für das Datenschutzrecht, ZD 2013, S. 562-568.

Rule/Ambady/Hallett, Female sexual orientation is perceived accurately, rapidly, and automatically from the face and its features, Journal of Experimental Social Psychology 2009, S. 1245-1251.

Simo, Big Data: Opportunities and Privacy Challenges, in: Roßnagel (Hrsg.), Privatheit, Öffentlichkeit und demokratische Willensbildung in Zeiten von Big Data, Baden-Baden 2015.

Solberg, Data Mining on Facebook: A Free Space For Researchers Or An IRB Nightmare?, Journal of Law, Technology & Policy 2010, S. 311-343.

Stoicescu, Big Data, the perfect instrument to study today's consumer behavior, Database Systems Journal 2015, Vol. VI, no. 3, S. 28-42.

Weichert, Big Data und Datenschutz Chancen und Risiken einer neuen Form der Datenanalyse, ZD 2013, S. 251-260.

Wolf, Big Data und Innere Sicherheit, Marburg 2015.

Youyou/Kosinski/Stillwell, Computer-based personality judgments are more accurate than those made by humans, PNAS 2015, S. 1036-1040.

G. Ich sammele, also bin ich (Social Credit) – Das Szenario eines allumfassenden Bonitätssystems am Beispiel Chinas (Barbara Kolany-Raiser und Tristan Radtke[1])

Stand: Juni 2018

Abstract: Social Credit

In China wird in Pilotprojekten ein allumfassendes Bonitätssystem (Social Credit) getestet und für den landesweiten Einsatz vorbereitet. Jedem Bürger soll ein Score zugeteilt werden, um das Vertrauen in der Gesellschaft zu stärken. Der Score kann Auswirkungen auf den gesamten Alltag haben. Vergleichbare Modelle in Europa durch private Unternehmen sind an dem Datenschutzrecht – insbesondere der Datenschutz-Grundverordnung – zu messen, das strenge Anforderungen statuiert. Ein solches System wäre nur bei erheblicher Kooperationsbereitschaft der Nutzer realisierbar und muss Auskunftsrechte und Einwirkungsmöglichkeiten der Nutzer berücksichtigen.

I. „Zero“ in der Realität

Marc Elsberg beschreibt in seinem Thriller „Zero – Sie wissen, was du tust“ das Szenario des gläsernen Bürgers, dem anhand seines Verhaltens ein individueller Punktewert (Score) zugeordnet wird.

Man stelle sich vor, jedem Bürger (und jedem Unternehmen) würde ein Score zugeordnet. Der Score spiegelt die Zuverlässigkeit wider. Wer pünktlich seine Rechnungen bezahlt, gesunde Produkte im Internet bestellt oder auf die „richtigen“ Internetseiten zugreift, erhält eine bessere

[1] Für seine wertvollen fachlichen Anmerkungen und Hintergrundinformationen zu Social-Credit-Projekten in China danken wir unserem Kollegen Fu Yu, der für vier Monate als studentische Hilfskraft im ABIDA-Projekt gearbeitet hat.

Bewertung. Wer hingegen Unterhaltsansprüche nicht begleicht oder anderweitig negativ auffällt, erhält einen Score-Malus. Dieses Szenario geht über das klassische Scoring als Bonitätsbewertung hinaus, indem weit mehr als nur die eigene Zahlungshistorie einbezogen wird.

In der Volksrepublik China befinden sich Vorläufer eines Scoring-Systems seit einigen Jahren in der Testphase. Im Folgenden sollen diese Ansätze vorgestellt werden und zum Anlass genommen worden, die datenschutzrechtlichen Grenzen eines solchen Systems in Europa von nicht-staatlicher Seite aufzuzeigen.

II. Begriffsklärung

Im Rahmen des Datenschutzrechts definiert der deutsche Gesetzgeber in § 31 Abs. 1 Bundesdatenschutzgesetz in der ab dem 25.05.2018 geltenden Fassung (BDSG 2018) Scoring als „die Verwendung eines Wahrscheinlichkeitswerts über ein bestimmtes zukünftiges Verhalten einer natürlichen Person zum Zweck der Entscheidung über die Begründung, Durchführung oder Beendigung eines Vertragsverhältnisses mit dieser Person“. Bei dem sog. Social Scoring steht hingegen nicht die Kreditwürdigkeit einer Person, sondern ihre Meinungsmacht im Vordergrund. Diese wird anhand ihrer Aktivitäten in sozialen Netzwerken berechnet.[2]

Ein Score, der sowohl die Zahlungshistorie einer Person als auch ihre Aktivitäten in sozialen Netzwerken und weitere Daten einbezieht und nicht nur die Kreditwürdigkeit, sondern auch insgesamt die Zuverlässigkeit und die Persönlichkeit einer Person einstuft, geht über das klassische Scoring hinaus. Da nicht die Meinungsmacht im Vordergrund steht, kann auch nicht von Social Scoring im engeren Sinne gesprochen werden. Das in China getestete System wird oft als Sozialkredit-System[3] oder auch im Englischen als Social-Credit-System[4] bezeichnet. Auch diese Begrifflichkeit ist zumindest missverständlich. Social Credit ist eine ökonomische

---

2 Auer-Reinsdorff/Conrad/Hausen, § 36 Datenschutz der Telemedien, Rn. 198.

3 http://www.deutschlandfunk.de/sozialkredit-system-china-auf-dem-weg-in-die-it-diktatur.724.de.html?dram:article_id=395440 (zuletzt abgerufen: 11/2018).

4 http://www.bbc.com/news/world-asia-china-34592186 (zuletzt abgerufen: 11/2018).

Theorie in Anlehnung an Clifford Hugh Douglas, die sich positive Auswirkungen auf die Gesellschaft durch ein ausgewogeneres Wirtschaftssystem erhofft.[5] In Anlehnung an die in der Berichterstattung verwendete Begrifflichkeit wird freilich auch in diesem Beitrag von einem Social-Credit-System gesprochen. Damit ist die Berechnung und Zuordnung eines Scores für jeden Marktteilnehmer gemeint, wobei der Score (langfristig) auf Grundlage von Zahlungshistorie, Daten aus sozialen Netzwerken und weiteren Datenquellen, Auskunft über die Zuverlässigkeit und soziales, gesellschaftsadäquates Verhalten geben soll. Auch wenn gerade die Bewertung der Unternehmen in China zur Regulierung des Marktsystems von überragender Bedeutung sein kann,[6] konzentriert sich dieser Beitrag maßgeblich auf die Bewertung natürlicher Personen.

III. Social-Credit-Pilotprojekte in China

In China fehlte es lange an Möglichkeiten zur Einschätzung der Kreditwürdigkeit.[7] Die Zuverlässigkeit eines Einzelnen einzuschätzen fällt auch deshalb schwer, weil viele Chinesen kein Auto oder Haus haben und oft auch keine Kreditkarte verwenden.[8] In einer Umfrage 2013 gaben nur etwa 30 Prozent der Befragten an, Fremden zu vertrauen.[9] Dieses Vertrauensdefizit sowohl im privaten als auch geschäftlichen Umfeld in China erklärt, warum ein allumfassendes Scoring derart interessant sein kann: Ein Social-Credit-System soll die Grundlage für mehr Vertrauen untereinander in China legen. Da die Ausweisnummer als Identifikationsmerkmal beispielsweise bei jedem Ticketkauf für Flugzeug oder Bahn dient, lassen sich potentiell viele Aktivitäten leicht einem Bürger zuordnen.[10]

---

5 http://www.douglassocialcredit.com (zuletzt abgerufen: 11/2018).

6 Meissner, S. 4.

7 https://netzpolitik.org/2015/dystopia-wird-wirklichkeit-was-ist-dran-an-chinas-social-credit-system/ (zuletzt abgerufen: 11/2018).

8 http://www.bbc.com/news/world-asia-china-34592186 (zuletzt abgerufen: 11/2018).

9 https://qz.com/398955/china-plans-to-use-big-data-to-rank-citizens-and-instil-good-behavior/ (zuletzt abgerufen: 11/2018).

10 http://www.deutschlandfunk.de/sozialkredit-system-china-auf-dem-weg-in-die-it-diktatur.724.de.html?dram:article_id=395440 (zuletzt abgerufen: 11/2018).

In China gibt es kein umfassendes Datenschutzrecht, sondern lediglich einige Vorgaben etwa zu der Erhebung der Daten direkt beim Individuum und bezüglich Informationspflichten.[11] Den Pilotprojekten steht damit kein umfangreiches Datenschutzrecht entgegen, zumal sie vom chinesischen Staat selbst initiiert wurden.

Zum jetzigen Zeitpunkt werden acht Pilotprojekte von privaten Unternehmen in China durchgeführt.[12] Ein prominentes Pilotprojekt ist „Sesame Credit", ein Social-Credit-System der Ant Financial Services Group, einer Tochtergesellschaft der chinesischen Alibaba Group.[13] Die Plattformen des Konzerns, etwa das Aktionshaus Taobao und der Zahlungsdienst Alipay, haben insgesamt mehrere Hundert Millionen Nutzer und bieten damit eine breite Datengrundlage für Sesame Credit. Sesame Credit sichert zu, nur Daten registrierter Nutzer zu verarbeiten.[14]

Der Sesame-Credit-Score bewegt sich zwischen 350-950 Punkten und setzt sich aus fünf Datenkategorien zusammen: über den Zahlungsdienst Alipay getätigte Zahlungen, persönliche Daten des Nutzers, die Zuverlässigkeit bei Zahlungen von Rechnungen oder per Kreditkarte und die Anzahl der eigenen Freunde auf Alipay.[15] Daten von sozialen Netzwerken sollen demnach nicht einbezogen werden. Bei diesem Pilotprojekt hängt eine gute Bewertung maßgeblich von einer intensiven Nutzung des Zahlungsdienstes Alipay und den gekauften Produkten ab. Details über den Algorithmus und die Gewichtungen der einzelnen Datenquellen sind jedoch nicht bekannt.[16] Beispielsweise soll der Kauf ausgewählter Produkte,

---

11 Forgó/Helfrich/Schneider/Spies, Kapitel 4, Rn. 28 f.

12 http://www.bbc.com/news/world-asia-china-34592186 (zuletzt abgerufen: 11/2018).

13 https://www.wired.co.uk/article/chinese-government-social-credit-score-privacy-invasion (zuletzt abgerufen: 11/2018).

14 https://techcrunch.com/2015/01/27/data-from-alibabas-e-commerce-sites-is-now-powering-a-credit-scoring-service/ (zuletzt abgerufen: 11/2018).

15 https://qz.com/1097766/i-fixed-my-poor-sesame-credit-score-by-being-a-more-loyal-user-of-alibabas-wallet-app-alipay-in-china/ (zuletzt abgerufen: 11/2018).

16 http://www.bbc.com/news/world-asia-china-34592186 (zuletzt abgerufen: 11/2018).

z. B. von Windeln als Indiz für – als vertrauenswürdig eingestufte – Eltern, sich auf den Score auswirken können.[17]

Die Nutzer von Sesame Credit können sich ihren Score in einer App anzeigen lassen.[18] Die Kooperation mit der beliebten Dating-App Baihe gibt bereits einen Ausblick, wie sich der Score auch im Alltag des Einzelnen auswirken kann: Ein guter Sesame-Credit-Score erleichtert die Partnersuche über Baihe durch prominente Platzierung.[19] Nutzern mit über 700 oder 750 Punkten werden darüber hinaus VISA-Erleichterungen in Aussicht gestellt.[20] Bereits ab 600 Punkten kann der Nutzer auf ein Darlehenskontingent zurückgreifen, um in den Online-Shops der hinter Sesame Credit stehenden Unternehmen einzukaufen.[21]

Tencent, bekannt für den Messenger-Dienst WeChat, betreibt ebenfalls ein Social-Credit-System, wobei sich auch das Verhalten der eigenen Kontakte auf sozialen Netzwerken auf den eigenen Score auswirken können soll.[22]

Das wohl wichtigste Pilotprojekt wird in der Stadt Rongcheng seit 2014 durchgeführt.[23] Alle Bürger der Stadt beginnen mit dem Punktestand 1000. Dieser Score kann auf bis zu 1050 steigen oder jedoch auf unter 599 Punkte sinken. Ordnungswidrigkeiten, wie das Überfahren einer roten Ampel, können sich negativ auswirken. Auch die Zufriedenheit anderer mit der eigenen Arbeit kann sich negativ oder positiv auf den Punktewert auswirken. Zahlreiche Behörden steuern für die Bewertung Daten

---

17 http://www.abc.net.au/news/2018-03-31/chinas-social-credit-system-punishes-untrustworthy-citizens/9596204 (zuletzt abgerufen: 11/2018).

18 https://qz.com/1097766/i-fixed-my-poor-sesame-credit-score-by-being-a-more-loyal-user-of-alibabas-wallet-app-alipay-in-china/ (zuletzt abgerufen: 11/2018).

19 https://www.heise.de/ct/ausgabe/2018-2-Konformitaetserziehung-per-sozialem-Punktesystem-3929709.html (zuletzt abgerufen: 11/2018).

20 https://www.chinadailyasia.com/business/2015-06/09/content_15274221.html (zuletzt abgerufen: 11/2018).

21 https://www.wired.co.uk/article/chinese-government-social-credit-score-privacy-invasion (zuletzt abgerufen: 11/2018).

22 http://www.chinadaily.com.cn/business/tech/2015-08/08/content_21535587.htm (zuletzt abgerufen: 11/2018).

23 http://www.deutschlandfunk.de/sozialkredit-system-china-auf-dem-weg-in-die-it-diktatur.724.de.html?dram:article_id=395440 (zuletzt abgerufen: 11/2018).

aus Strafregistern, Informationen der Finanzbehörden und der staatlichen Telekommunikationsunternehmen bei.[24]

Bestbewertete werden bei der Zulassung für Schulen, dem Abschluss von Versicherungen und bei der Gewährung von sozialen Leistungen bevorzugt. Wer hingegen einen schlechten Score hat, muss mit Kürzungen von Sozialleistungen rechnen und mit deutlich schlechteren beruflichen Aufstiegschancen.

Bewohner Rongchengs berichten von einer vertrauenswürdigeren Atmosphäre. Das Social-Credit-System kann jedoch zu einem mächtigen Kontrollinstrument avancieren, zum Beispiel wenn kritische Äußerungen oder Petitionen in sozialen Netzwerken sich negativ im Punkte-System auswirken.[25] Sozialer Druck kann auch erzeugt werden, wenn das Verhalten von Freunden und Bekannten Auswirkungen auf den eigenen Score haben kann, wie etwa bisher bei dem Sesame-Credit-Pilotprojekt.[26]

Ein Pilotprojekt in der Stadt Suzhou folgt einem ähnlichen Konzept. Dort soll beispielsweise auch eine Blutspende oder ehrenamtliche Arbeit berücksichtigt werden.[27] Werden Bürger mit einem besonders schlechten Score angerufen, ertönt vor der Durchstellung eine Ansage, die auf den schlechten Score hinweist.[28]

Auch die Stadtregierung der Millionen-Stadt Shanghai setzt eine App ein, um das Verhalten ihrer Bürger zu bewerten.[29]

Darüber hinaus wurde bereits 2015 eine nationale Plattform für den Austausch der Bonitätsinformationen ins Leben gerufen, die bisher allerdings

---

24 https://www.swr.de/swr2/programm/sendungen/wissen/china-it-diktatur/-/id=660374/did=20878286/nid=660374/1caeff2/index.html (zuletzt abgerufen: 11/2018).

25 http://www.deutschlandfunk.de/sozialkredit-system-china-auf-dem-weg-in-die-it-diktatur.724.de.html?dram:article_id=395440 (zuletzt abgerufen: 11/2018).

26 https://netzpolitik.org/2015/dystopia-wird-wirklichkeit-was-ist-dran-an-chinas-social-credit-system/ (zuletzt abgerufen: 11/2018).

27 http://www.abc.net.au/news/2018-03-31/chinas-social-credit-system-punishes-untrustworthy-citizens/9596204 (zuletzt abgerufen: 11/2018).

28 http://www.abc.net.au/news/2018-03-31/chinas-social-credit-system-punishes-untrustworthy-citizens/9596204 (zuletzt abgerufen: 11/2018).

29 https://www.swr.de/swr2/programm/sendungen/wissen/china-it-diktatur/-/id=660374/did=20878286/nid=660374/1caeff2/index.html (zuletzt abgerufen: 11/2018).

nur überwiegend staatlich gesammelte Informationen, und zwar hauptsächlich solche zu Unternehmen, zusammenführt.[30]

IV. Ausblick auf Social Credit in China

Ein Plan der chinesischen Regierung sieht vor, ab 2020 ein staatliches Social-Credit-System einzuführen.[31] Demnach soll ab 2020 jedem Volljährigen der 1,3 Mrd. Bürger ein Social Score zugeteilt werden.[32] Unternehmen sollen einen separaten Score erhalten,[33] auf den sich beispielsweise auch Verstöße gegen Emissionsvorgaben oder andere Vorschriften auswirken können.[34] Aufgrund der engen Zusammenarbeit der chinesischen IT-Unternehmen, wie Alibaba und Baidu, ist davon auszugehen, dass auch gesammelte Daten genannter Unternehmen in einen Social Score einfließen werden.[35] Das hätte zur Folge, dass auch Internet-Suchanfragen und Online-Einkäufe Auswirkungen auf die Punkte-Bewertung haben können. Denkbar ist darüber hinaus auch, das Verhalten der Bürger in der Öffentlichkeit durch moderne Gesichtserkennungssoftware der Videokameras zu erfassen, zumal diese flächendeckend in chinesischen Großstädten installiert werden sollen.[36]

Neben den Pilotprojekten lässt der Plan erahnen, welche Auswirkungen der Score haben kann. Die Einführung einer Online Black List wird angedacht, um Bürger mit schlechtem Score von Dienstleistungen auszuschließen.[37] Daneben werden über Sanktionen wie einen langsameren

---

30 Meissner, S. 8.

31 Englische Übersetzung des Plans GF No. (2014)21 zu finden unter: https://chinacopyrightandmedia.wordpress.com/2014/06/14/planning-outline-for-the-construction-of-a-social-credit-system-2014-2020/ (zuletzt abgerufen: 11/2018).

32 https://www.volkskrant.nl/buitenland/china-rates-its-own-citizens-including-online-behaviour~a3979668/ (zuletzt abgerufen: 11/2018).

33 http://www.bjreview.com.cn/nation/txt/2014-07/25/content_630381.htm (zuletzt abgerufen: 11/2018).

34 Meissner, S. 4.

35 https://www.volkskrant.nl/buitenland/china-rates-its-own-citizens-including-online-behaviour~a3979668/ (zuletzt abgerufen: 11/2018).

36 http://www.zeit.de/digital/datenschutz/2017-11/china-social-credit-system-buerger bewertung/komplettansicht (zuletzt abgerufen: 11/2018).

37 Vgl. die erwähnte englische Übersetzung des Plans GF No. (2014)21: „Establish online credit black list systems, list enterprises and individuals engaging in online

Internetzugang, eingeschränkten Zugang zu Restaurants und Clubs sowie schlechtere berufliche Perspektiven spekuliert.[38] Bereits 2017, vor der Einführung eines nationalen Social-Credit-Systems, sollen mehrere Millionen Bürger von der Buchung von Flugzeug- oder gar Bahn-Tickets oder Hotel-Übernachtungen in Sterne-Hotels ausgeschlossen worden sein.[39]

Ob und in welchem Umfang ein solches Social-Credit-System tatsächlich realisiert wird, wird sich zeigen. Bis zur Einführung soll es nach Aussagen eines Beteiligten noch einige Probleme zu lösen geben.[40] Die tatsächliche Einführung würde auch Antworten auf Fragen wie diese mit sich bringen: Werden Minderjährige, ausländische Staatsangehörige oder ausländische Unternehmen ebenfalls bewertet? Wobei sich bereits festhalten lässt, dass der Plan der chinesischen Regierung nicht zwischen inländischen und ausländischen Unternehmen unterscheidet. Es gilt daher als wahrscheinlich, dass ausländische Unternehmen ebenfalls bewertet werden.[41]

Welche Datenquellen werden tatsächlich herangezogen? Welche Konsequenzen hat ein guter oder schlechter Score im Alltag? Wird das Social-Credit-System maßgeblich zur Schaffung von Vertrauen in der Gesellschaft und Wirtschaft verwendet oder steht die Stärkung der Kontrolle über etwaige Dissidenten im Vordergrund?

---

swindles, rumourmongering, infringement of other persons' lawful rights and interests and other grave acts of breaking trust online onto black lists, adopt measures against subjects listed on black lists including limitation of online conduct and barring sectoral access, and report them to corresponding departments for publication and exposure".

38 https://www.wired.co.uk/article/chinese-government-social-credit-score-privacy-invasion (zuletzt abgerufen: 11/2018).

39 https://www.wired.co.uk/article/chinese-government-social-credit-score-privacy-invasion (zuletzt abgerufen: 11/2018); http://www.abc.net.au/news/2018-03-31/chinas-social-credit-system-punishes-untrustworthy-citizens/9596204 (zuletzt abgerufen: 11/2018).

40 http://www.abc.net.au/news/2018-03-31/chinas-social-credit-system-punishes-untrustworthy-citizens/9596204 (zuletzt abgerufen: 11/2018).

41 Meissner, S. 11.

V. Social Credit in Deutschland und Europa?

Das Scoring, die Entscheidung über einen Vertragsschluss anhand eines Wahrscheinlichkeitswerts bzw. einer Bewertung der Kreditwürdigkeit und Zuverlässigkeit der Person, ist schon lange in großen Industriestaaten wie den USA und auch in Europa angekommen. In den USA etwa werden schon seit Jahrzehnten sog. FICO Scores eingesetzt.[42] Der europäische Gesetzgeber sah schon 1995 bei Erlass der Datenschutz-Richtlinie 95/46/EG Regelungsbedarf zum Schutz vor sog. automatisierten Entscheidungen, vgl. Art. 15 RL 95/46/EG. Die Datenschutz-Grund-Verordnung (DS-GVO[43]), die seit dem 25.05.2018 gilt, sieht ebenfalls entsprechende Regelungen vor. Auskunfteien, die Wahrscheinlichkeitswerte zur Kreditwürdigkeit bereitstellen, wie etwa die Schufa Holding AG in Deutschland, sind längst nicht mehr unbekannt. Aufgrund der immer populäreren Onlineplattformen und den diesen zur Verfügung stehenden Datenmengen ist besonders ein Szenario aus datenschutzrechtlicher Sicht interessant: Unter welchen Voraussetzungen können Unternehmen in Europa unter der DS-GVO ein eigenes Social-Credit-System aufbauen, d.h. jedem Kunden einen Score zuteilen, der nicht nur auf einer Bestellhistorie fußt, sondern auch Daten von anderen Plattformen einbezieht und zur Entscheidungsgrundlage über Vertragsabschlüsse wird.

Für ein solches Szenario sind der räumliche und sachliche Anwendungsbereich der DS-GVO, die Datenerhebung und -übermittlung zwischen Unternehmen – gegebenenfalls auch innerhalb einer Unternehmensgruppe – sowie die Verwendung zur automatisierten Entscheidungsfindung maßgeblich. Daneben ist das deutsche BDSG 2018 zu berücksichtigen.

---

42 https://www.wired.co.uk/article/chinese-government-social-credit-score-privacy-invasion (zuletzt abgerufen: 11/2018).

43 Soweit nachfolgend Erwägungsgründe zitiert werden, sind diese solche der DS-GVO.

1. Räumlicher und sachlicher Anwendungsbereich der DS-GVO

Seit dem 25.05.2018 gilt die DS-GVO unmittelbar in jedem Mitgliedstaat. Nach dem sachlichen Anwendungsbereich ist nahezu jeder (teil-)automatisierte Vorgang mit Bezug zu personenbezogenen Daten als Verarbeitung umfasst, Art. 2 Abs. 1, Art. 4 Nr. 2 DS-GVO. Personenbezogene Daten sind nach Art. 4 Nr. 1 DS-GVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Jegliche Information, die einer natürlichen Person zugeordnet wird und zur softwaregestützten Berechnung eines Scores für diese Person verwendet wird, ist damit ein solches personenbezogenes Datum. Soweit allerdings juristischen Personen ein Score ohne einen Bezug zu einer dahinterstehenden natürlichen Person zugeordnet wird, fällt der Vorgang nicht in den sachlichen Anwendungsbereich. Bei der „Ein-Mann-GmbH“ als juristische Person wird sich etwa im Regelfall ein Bezug zu einer dahinterstehenden natürlichen Person herstellen lassen.[44]

Für die Eröffnung des räumlichen Anwendungsbereichs muss die Verarbeitung nicht einmal im Rahmen der Tätigkeiten einer Niederlassung erfolgen, Art. 3 Abs. 1 DS-GVO. Es ist bereits ausreichend nach Art. 3 Abs. 2 DS-GVO, wenn Personen, die sich in der Union befinden, Waren oder Dienstleistungen angeboten werden sollen oder deren Verhalten beobachtet werden soll.

2. Datenübermittlung zwischen Unternehmen und Zusammenführung zur Berechnung eines Scores als Verarbeitung

Für einen Social-Credit-Ableger eines europäischen Unternehmens wäre es von entscheidender Bedeutung, Daten zu einer Person aus mehreren Datenquellen unterschiedlicher Unternehmen zusammenzuführen. Sowohl die Übermittlung als auch die Zusammenführung der personenbezogenen Daten mehrerer Unternehmen zur Score-Berechnung stellen eine solche Verarbeitung dar, vgl. Art. 4 Nr. 2 DS-GVO. Die Verarbeitung

---

44 Gola, Art. 4, Rn. 24.

ist jeweils nur zulässig, wenn einer der Erlaubnistatbestände des Art. 6 Abs. 1 DS-GVO greift.

Da bei einem Social-Credit-System spätestens die automatisierte Übermittlung erfolgt, „um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich […] wirtschaftliche Lage […] [oder] Zuverlässigkeit […] vorherzusagen“ handelt es sich um die besondere Verarbeitungssituation des sog. Profilings nach Art. 4 Nr. 4 DS-GVO.

Neben der Frage der Rechtmäßigkeit der Verarbeitung nach Art. 6 Abs. 1 DS-GVO und der Einhaltung der Grundsätze aus Art. 5 DS-GVO sind daher weitergehende Pflichten und Betroffenen-Rechte zu berücksichtigen.

a) Reichweite des Zwecks (Art. 6 Abs. 4 DS-GVO)

Die Übermittlung der ursprünglich bei Unternehmen, wie Online-Shops oder sozialen Netzwerken, verarbeiteten Daten, könnte unter Umständen nach Art. 6 Abs. 4 DS-GVO keines weiteren Erlaubnistatbestands bedürfen.[45] Insoweit ist Art. 6 Abs. 4 DS-GVO unter Berücksichtigung der Gesetzgebungshistorie als (erweiterte) Auslegungsregel für die Reichweite des ursprünglichen Zwecks zu verstehen.[46]

Soweit der ursprüngliche Verarbeitungszweck nicht mehr die Übermittlung und Zusammenführung zum Zwecke eines Social-Credit-Systems umfasst, kommt die Zulässigkeit unter Berücksichtigung des Art. 6 Abs. 4 DS-GVO in Betracht. Im Rahmen einer Interessenabwägung[47] sind unter anderem die Folgen für den Betroffenen und eine Verbindung zwischen dem ursprünglichen und dem nunmehr relevanten Zweck zu berücksichtigen. Die Übermittlung der von sozialen Netzwerken im Rahmen einer Einwilligung verarbeiteten Daten lässt sich demnach nicht auf Art. 6 Abs. 4 DS-GVO stützen. Die Übermittlung an ein zentrales Social-Credit-Unternehmen um dem Betroffenen einen Score zuzuweisen, geht nämlich in derartigen Fällen über den ursprünglichen Zweck hinaus und ist

---

45 Vgl. Erwägungsgrund 50: „[…] wenn die Verarbeitung mit den Zwecken, für die die personenbezogenen Daten ursprünglich erhoben wurden, vereinbar ist, […] ist keine andere gesonderte Rechtsgrundlage erforderlich“.

46 Kühling/Buchner/Petri, Art. 6, Rn. 183.

47 Plath, Art. 6, Rn. 38.

angesichts der erheblichen Folgen eines solchen Scorings – vgl. Art. 22 DS-GVO – nicht mehr nach Art. 6 Abs. 4 DS-GVO zulässig.

Daher stellt sich die Frage, inwieweit sich die Übermittlung und Zusammenführung auf die Erlaubnistatbestände aus Art. 6 Abs. 1 DS-GVO stützen lässt.

b) Einwilligung (Art. 6 Abs. 1 UA 1 lit. a DS-GVO)

Als Erlaubnistatbestand kommt die Einwilligung der betroffenen Person für die jeweiligen Zwecke der Verarbeitung nach Art. 6 Abs. 1 UA 1 lit. a, Art. 4 Nr. 11 DS-GVO in Betracht. Die Zwecke sind dabei konkret zu bezeichnen.[48] Eine Blanko-Einwilligung durch einen äußerst weit formulierten Zweck ist nicht möglich.[49]

Die Einwilligung unterliegt im Hinblick auf die Form des Ersuchens und der Freiwilligkeit nach Art. 7 Abs. 2 und 4 DS-GVO nicht zu unterschätzenden Anforderungen.[50] Insbesondere kann der Freiwilligkeit entgegenstehen, dass die Erfüllung eines Vertrags von der Einwilligung abhängig gemacht wird („Kopplungsverbot“), Art. 7 Abs. 4 DS-GVO.[51] Sollte beispielsweise ein Online-Shop nur Kunden den Einkauf ermöglichen, die in eine Übermittlung für ein umfassendes Scoring eingewilligt haben, steht die Freiwilligkeit der Einwilligung in Zweifel. Strengere Anforderungen gelten im Übrigen gegenüber Kindern unter 16 Jahren nach Art. 7, 8 DS-GVO.

Die Einwilligung kann nach Art. 7 Abs. 3 DS-GVO mit Wirkung für die Zukunft widerrufen werden. Soweit ab Widerruf keine andere Rechtsgrundlage oder Ausnahme nach Art. 17 Abs. 3 DS-GVO, vgl. auch § 35 BDSG

---

48 Vgl. Erwägungsgrund 32: „Die Einwilligung sollte durch eine eindeutige bestätigende Handlung erfolgen, mit der freiwillig, für den konkreten Fall, in informierter Weise und unmissverständlich bekundet wird, dass die betroffene Person mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist […]“.

49 Gola/Schulz, Art. 6, Rn. 23.

50 Art. 29 Datenschutzgruppe, Guidelines on Consent under Regulation 2016/679, S. 9 f.

51 Vgl. auch Erwägungsgrund 43: „Die Einwilligung gilt als nicht freiwillig erteilt, wenn […] die Erfüllung eines Vertrags […] von der Einwilligung abhängig ist, obwohl diese Einwilligung für die Erfüllung nicht erforderlich ist.“

2018, für die Fortsetzung der Speicherung einschlägig ist, kann der Betroffene darüber hinaus auch Löschung der personenbezogenen Daten verlangen, Art. 17 Abs. 1 lit. b DS-GVO. In einem solchen Fall müssten also die jeweils übermittelten personenbezogenen Daten gelöscht werden. Bei einem Widerruf gegenüber dem Unternehmen, das die Daten an ein anderes übermittelt hat, hat ersteres außerdem das Unternehmen, an das die Daten übermittelt wurden, nach Art. 19 S. 1 DS-GVO über die Löschung zu informieren.

c) Vertragserfüllung (Art. 6 Abs. 1 UA 1 lit. b DS-GVO)

Nach Art. 6 Abs. 1 UA 1 lit. b DS-GVO ist eine Verarbeitung rechtmäßig, soweit sie für die Erfüllung eines Vertrags erforderlich ist. Wobei die Erforderlichkeit eng auszulegen ist,[52] jedoch nicht mit Unverzichtbarkeit gleichzusetzen ist.[53] In Anlehnung an das chinesische Vorbild wäre folgende Konstellation denkbar: Die Nutzer schließen einen Vertrag mit einem Social-Credit-Unternehmen. Hauptleistungspflicht seitens des Unternehmens ist die Berechnung eines Scores, mit dem der Nutzer wiederum bei anderen Unternehmen einen Vorteil erhält. Für die Erfüllung dieser Pflicht wäre die Zusammenführung von Daten für die Berechnung eines Scores, je nach Ausgestaltung des Vertrags, erforderlich und damit rechtmäßig. Ein derartiger Vertragsschluss ist als Ausdruck der Privatautonomie zulässig. In der Vergangenheit wurde bereits die Datenübermittlung von Payback-Partnern an das Bonussystem Payback als erforderlich für die Durchführung des Vertragsverhältnisses erachtet.[54] Entscheidend ist, dass sich der Nutzer autonom für den Abschluss eines solchen Vertrags entschieden hat.[55] Dann kommt der Rechtmäßigkeitstatbestand für die Tätigkeit des Social-Credit-Dienstleisters in Betracht, soweit die

---

52 Art. 29 Datenschutzgruppe, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, S. 13.

53 BGH, Urteil vom 16.07.2008 – VIII ZR 348/06, MMR 2008, S. 731, 735.

54 BGH, Urteil vom 16.07.2008 – VIII ZR 348/06, MMR 2008, S. 731, 735.

55 Kühling/Buchner/Petri, Art. 6, Rn. 30.

Verarbeitung konkret für diesen Vertragszweck erforderlich ist. Maßgeblich kommt es also auf die Auslegung des geschlossenen Vertrags und die vereinbarten leistungsbezogenen Pflichten an.[56]

In Konstellationen, in denen Gratis-Dienstleistungen, finanziert durch datengestützt optimierte Werbung, angeboten werden, ist unklar, ob das Vertragsrecht ausreichend schützt[57] oder ob die Anforderungen an die Einwilligung vorrangig sind.[58]

Praktisch würde jedoch der Nutzer, der bereits mit einem solchen Geschäftsmodell einverstanden ist, wohl auch seine Einwilligung erteilen. An dieser Stelle stellt sich hingegen die Frage, welche Nutzer tatsächlich zu einem solchen Vertragsschluss bereit wären.

d) Wahrung berechtigter Interessen (Art. 6 Abs. 1 UA 1 lit. f DS-GVO)

Als eine andere Rechtsgrundlage für die Übermittlung kommt die Wahrung berechtigter Interessen in Betracht, sofern nicht die Interessen der betroffenen Person überwiegen – unter anderem denkbar bei Kindern als Betroffenen –, Art. 6 Abs. 1 UA 1 lit. f DS-GVO. Nach Erwägungsgrund 48 kann insbesondere die Übermittlung innerhalb einer Unternehmensgruppe für interne Verwaltungszwecke ein solches berechtigtes Interesse darstellen.[59] Soweit die verschiedenen Unternehmen eines Konzerns gegenüber dem Kunden einheitlich auftreten und diesem ein einheitliches Kundenprofil mit einem Score zuweisen, könnte darin im Einzelfall ein berechtigtes Interesse zu sehen sein. Unabhängig davon ist jedoch immer die Erforderlichkeit dieses Scores zu beachten, Art. 5 Abs. 1 lit. b, c

---

56 BGH, Urteil vom 28.10.2014 – X ZR 79/13, NJW 2015, S. 687.

57 Schantz/Wolff, Rn. 544.

58 Kühling/Buchner/Petri, Art. 6, Rn. 41.

59 Erwägungsgrund 48: „Verantwortliche, die Teil einer Unternehmensgruppe oder einer Gruppe von Einrichtungen sind, die einer zentralen Stelle zugeordnet sind können ein berechtigtes Interesse haben, personenbezogene Daten innerhalb der Unternehmensgruppe für interne Verwaltungszwecke, einschließlich der Verarbeitung personenbezogener Daten von Kunden und Beschäftigten, zu übermitteln. Die Grundprinzipien für die Übermittlung personenbezogener Daten innerhalb von Unternehmensgruppen an ein Unternehmen in einem Drittland bleiben unberührt.“

und e DS-GVO (vgl. die Ausführungen zur Übermittlung an Unternehmen außerhalb einer Unternehmensgruppe unten).

Wann immer, selbst innerhalb einer Unternehmensgruppe, personenbezogene Daten in Drittländer übermittelt werden, sind die Art. 44 ff. DS-GVO zu beachten. So soll sichergestellt werden, „dass das durch diese Verordnung gewährleistete Schutzniveau für natürliche Personen nicht untergraben wird“, Art. 44 S. 2 DS-GVO. Drittländer sind dabei solche Länder, in denen die DS-GVO nicht gilt,[60] und damit zum jetzigen Zeitpunkt auch noch die EFTA-Staaten[61]. Innerhalb einer Unternehmensgruppe sind durch die zuständige Aufsichtsbehörde genehmigte, verbindliche interne Datenschutzvorschriften (Binding Corporate Rules) nach Art. 47 DS-GVO ein probates Mittel.

Für eine Übermittlung an Unternehmen außerhalb einer Unternehmensgruppe, etwa in Form einer Kooperation mehrerer Internetplattformen wie Online Shops und sozialer Netzwerke, müsste hingegen ein gesondertes berechtigtes Interesse bestehen. Bloße Allgemeininteressen, wie im Beispiel China die Stärkung von Vertrauen in der Gesellschaft, sind nicht ausreichend.[62] Das zeigt in systematischer Hinsicht auch der Umkehrschluss aus Art. 6 Abs. 1 UA 1 lit. e DS-GVO. Alle beteiligten Unternehmen haben ein wirtschaftliches Interesse daran, in einem auf umfassender Datengrundlage berechneten Score die Zuverlässigkeit des Kunden unter anderem im Hinblick auf zukünftige Bestellungen vorherzusagen und aus diesem Grund Daten zu übermitteln und zusammenzuführen. Dieses Interesse ähnelt dem in Erwägungsgrund 47 beispielhaft genannten bei der Verhinderung von Betrug[63] und lässt sich auch auf Art. 16 Abs. 1 Grundrechte-Charta (GRCh) stützen, sodass es ein berechtigtes

---

60 Paal/Pauly, Art. 44, Rn. 6.

61 Siehe zum Stand der Übernahme durch die EFTA-Staaten: http://www.efta.int/eea-lex/32016R0679 (zuletzt abgerufen: 11/2018).

62 Kühling/Buchner/Petri, Art. 6, Rn. 146.

63 Erwägungsgrund 47: „[…] Die Verarbeitung personenbezogener Daten im für die Verhinderung von Betrug unbedingt erforderlichen Umfang stellt ebenfalls ein berechtigtes Interesse des jeweiligen Verantwortlichen dar. […]“

Interesse darstellt. Auch der Betroffene selbst kann ein Interesse an einem Schutz vor Überschuldung und Zahlungsunfähigkeit haben.[64]

Soweit die zugrunde liegenden Daten unrichtig sind, überwiegen stets die Interessen des Betroffenen.[65]

Ein umfassendes Scoring in Form eines Social-Credit-Systems beeinträchtigt mangels Erforderlichkeit, vgl. Art. 52 Abs. 1 S. 2 GRCh, das Recht des Betroffenen auf den Schutz personenbezogener Daten nach Art. 8 Abs. 1 GRCh derart stark, dass die Interessen der betroffenen Person überwiegen und die Rechtsgrundlage des Art. 6 Abs. 1 UA 1 lit. f DS-GVO insoweit ausscheidet. Zwar besteht an Daten über konkrete Zahlungsabwicklungen in der Vergangenheit ein größeres Interesse und eine solche Datenzusammenführung kann deshalb noch zu rechtfertigen sein.[66] Soweit sich aus anderen Daten typischerweise Aussagen über das Zahlungsverhalten treffen lassen, kann auch insoweit ein berechtigtes Interesse bestehen, dem nicht überwiegende Interessen des Nutzers gegenüberstehen.[67] Werden allerdings, wie zum Teil im chinesischen Social-Credit-System beabsichtigt, auch Daten über die Zuverlässigkeit des Nutzers bei seiner Arbeit oder im Alltag oder aber anhand von Likes und Posts in sozialen Netzwerken zusammengetragen und in die Bewertung einbezogen, dürften diese Daten typischerweise nicht mehr zur Aussage über das zukünftige Zahlungsverhalten geeignet sein. Zumindest überwiegt angesichts der umfangreichen Zusammentragung nach dem Grundsatz der Erforderlichkeit der Daten das Interesse des Betroffenen.

Die Übermittlung und Zusammenführung von Daten, die „auf Verdacht“ in irgendeiner Form etwas über die Zuverlässigkeit der Person aussagen könnten, kann also im Regelfall nicht auf Art. 6 Abs. 1 UA 1 lit. f DSG-VO gestützt werden.

---

64 Taeger, ZRP 2016, S. 72, 74.

65 Kühling/Buchner/Petri, Art. 6, Rn. 151.

66 Gola/Schulz, Art. 6, Rn. 139.

67 Gola/Schulz, Art. 6, Rn. 139.

e) Besondere Anforderungen an die Verarbeitung besonderer Kategorien persönlicher Daten (Art. 9 DS-GVO)

Soweit nach Art. 9 Abs. 1 DS-GVO genetische Daten oder Daten zur Score-Berechnung herangezogen werden, „aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen", unterliegt die Verarbeitung erhöhten Anforderungen. Es reicht aus, wenn diese besonderen Informationen mittelbar aus den Daten hervorgehen[68] – etwa wenn sich anhand einer Korrelation mit einer gewissen Wahrscheinlichkeit aufgrund anderer Daten beispielsweise die politische Einstellung vermuten lässt. Allerdings muss eine Auswertungsabsicht bestehen[69] bzw. es bedarf zumindest einer genauen Untersuchung der Verarbeitung im Einzelfall.[70] Ein Social-Credit-System, das anhand der gesammelten Daten auch Mutmaßungen z. B. zu politischen Meinungen anstellen könnte oder derartige Korrelationen für den Score berücksichtigen könnte, dies aber nicht tut, muss sich insoweit nach hier vertretener Auffassung nicht an Art. 9 DS-GVO messen lassen.

Andernfalls ist die Verarbeitung nach Art. 9 Abs. 1 DS-GVO unzulässig, wenn nicht eine der Ausnahmen in Art. 9 Abs. 2 DS-GVO, vgl. auch §§ 22, 27 f. BDSG 2018, einschlägig ist. Daneben muss weiterhin ein allgemeiner Erlaubnistatbestand aus Art. 6 Abs. 1 DS-GVO greifen,[71] was vereinzelt anders gesehen wird.[72]

---

68 Kühling/Buchner/Weichert, Art. 9, Rn. 24; Art. 29 Datenschutzgruppe, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, S. 15.

69 Gola/Schulz, Art. 9, Rn. 11.

70 Kühling/Buchner/Weichert, Art. 9, Rn. 24.

71 Art. 29 Datenschutzgruppe, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, S. 15; vgl. auch Erwägungsgrund 51: „[…] Zusätzlich zu den speziellen Anforderungen an eine derartige Verarbeitung [besonderer Kategorien personenbezogener Daten] sollten die allgemeinen Grundsätze […], insbesondere hinsichtlich der Bedingungen für eine rechtmäßige Verarbeitung, gelten […]".

72 Ehmann/Selmayr/Schiff, Art. 9, Rn. 9.

In Betracht kommt nach Art. 9 Abs. 2 lit. a DS-GVO die Einwilligung, welche sich jedoch explizit auf die Verarbeitung solcher besonders persönlichen Daten beziehen muss.[73] Im Falle von sozialen Netzwerken und Nutzerprofilen, die der Nutzer entsprechend der Einstellungsmöglichkeiten selbst öffentlich gemacht hat, greift Art. 9 Abs. 2 lit. e DS-GVO.

Bei einer umfangreichen Verarbeitung solcher Daten ist nach Art. 35 Abs. 3 lit. b DS-GVO eine Datenschutz-Folgeabschätzung und nach § 38 Abs. 1 S. 2 BDSG 2018, vgl. Öffnungsklausel in Art. 37 Abs. 4 S. 1 Hs. 2 DS-GVO, die Benennung eines Datenschutzbeauftragten erforderlich.

Außerdem ist die Verarbeitung besonderer Kategorien persönlicher Daten als Umstand im Rahmen der Reichweite des Zwecks nach Art. 6 Abs. 4 DS-GVO zu berücksichtigen.

f) Betroffenen-Rechte im Allgemeinen und im Besonderen bei Verarbeitungen zu Profiling-Zwecken

Die Datenübermittlung und Zusammenführung zu Zwecken der Bewertung der Zuverlässigkeit anhand eines Scores ist nach Art. 4 Nr. 4 DS-GVO, wie gezeigt, Profiling als eine besondere Form der Verarbeitung.[74] Für ein Social-Credit-System sind daher weitergehende Anforderungen zu beachten. Insbesondere ist schon nach Art. 35 Abs. 3 lit. a DS-GVO stets eine Datenschutz-Folgeabschätzung erforderlich, da ein Social-Credit-System der systematischen und umfassenden Bewertung persönlicher Aspekte natürlicher Personen auf Grundlage von Profiling dient und der Score seinerseits Grundlage für spätere automatisierte Entscheidungen ist. Damit muss auch ein Datenschutzbeauftragter nach § 38 Abs. 1 S. 2 BDSG 2018 benannt werden.

Neben den allgemeinen Informationspflichten nach Art. 13 f. DS-GVO sind dem Betroffenen beim Profiling zum Zwecke der automatisierten Entscheidungsfindung nach Art. 13 Abs. 2 lit. f DS-GVO bzw. Art. 14 Abs. 2 lit. g DS-GVO Informationen über „das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Art. 22

---

73 Gola/Schulz, Art. 9, Rn. 4.

74 Kühling/Buchner, Art. 22, Rn. 22.

Abs. 1 und 4 und – zumindest in diesen Fällen – aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person“ zur Verfügung zu stellen. Diese Informationen sind auch im Rahmen eines Auskunftsverlangens des Betroffenen nach Art. 15 Abs. 1 lit. h DS-GVO zur Verfügung zu stellen. Informationen über die involvierte Logik umfassen dabei nicht die Offenlegung des gesamten Algorithmus.[75] Außerdem besteht kein Anspruch auf Berechnung des Scores, falls ein solcher bis dato noch nicht berechnet und gespeichert wurde.[76] Ungeachtet dessen kann sich aus dem Vertrag zwischen Social-Credit-Unternehmen und Nutzer ein solcher Anspruch auf Score-Berechnung ergeben.

Art. 21 Abs. 1 S. 1 Hs. 2 DS-GVO stellt zudem deklaratorisch klar, dass sich das Widerspruchsrecht auch auf Profiling bezieht. Bei Gründen, die sich aus der besonderen Situation des Betroffenen ergeben, kann die Einstellung der Verarbeitung der personenbezogenen Daten auf Grundlage berechtigter Interessen (Art. 6 Abs. 1 UA 1 lit. f DS-GVO) erreicht werden. Nur wenn zwingende schutzwürdige Gründe für die Verarbeitung überwiegen, darf sie fortgesetzt werden. Dabei trägt der Verantwortliche die Beweislast, was gegenüber Art. 6 Abs. 1 UA 1 lit. f DS-GVO erhöhte Anforderungen darstellt.[77] Bis zur Klärung kann der Betroffene nach Art. 18 Abs. 1 lit. d, 2 DS-GVO die Beschränkung der Verarbeitung auf die bloße Speicherung verlangen.

Die Anforderungen an die Gründe, die sich aus der besonderen Situation des Betroffenen ergeben, sind unklar. Nach Art. 21 Abs. 5 DS-GVO kann das Widerspruchsrecht bei der Nutzung von Diensten der Informationsgesellschaft auch mittels automatisierter technischer Verfahren ausgeübt werden. Das legt angesichts von Funktionen wie dem „Do Not Track“-

---

75 Art. 29 Datenschutzgruppe, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, S. 25; Ehmann/Selmayr, Art. 15, Rn. 16.

76 Gola/Franck, Art. 15, Rn. 16.

77 Vgl. Erwägungsgrund 69: „[…] Der für die Verarbeitung Verantwortliche sollte darlegen müssen, dass seine zwingenden berechtigten Interessen Vorrang vor den Interessen oder Grundrechten und Grundfreiheiten der betroffenen Person haben.“

Header,[78] welcher keine Informationen über die spezifische Situation der Person enthält, nahe, niedrige Anforderungen an diese Gründe zu stellen.[79] Andererseits findet bereits im Rahmen des Art. 6 Abs. 1 UA 1 lit. f DS-GVO eine Interessenabwägung statt,[80] die im Falle niedriger Anforderungen unterlaufen werden würde.

Unabhängig von den zu stellenden Anforderungen, ermöglicht die Einlegung des Widerspruchs auch mittels eines technischen Verfahrens zumindest erst einmal die Einschränkung der Verarbeitung, Art. 18 Abs. 1 lit. d, 2 DS-GVO.

Gerade im Hinblick auf die Berechnung eines Scores haben die Betroffenen ein besonderes Interesse daran, ihren Score möglichst korrekt berechnet zu wissen. Auch wenn ein solcher Score eine Wertung enthält,[81] kann der Betroffene nach Art. 16 S. 1 DS-GVO Berichtigung verlangen, wenn sich der Score als unrichtig darstellt, vgl. Art. 5 Abs. 1 lit. d DS-GVO.[82] Diese Möglichkeit der Berichtigung steht dem Betroffenen etwa bei Berechnung des Scores auf Grundlage veralteter oder falscher Daten zu.[83] Da hinsichtlich der Vollständigkeit der Verarbeitungszweck zu berücksichtigen ist[84] und das Social-Credit-Portal in der Regel von vornherein nur Daten ausgewählter Portale berücksichtigen wird, kann der Betroffene nicht nach Art. 16 S. 2 DS-GVO verlangen, dass beispielsweise auch die Daten seiner Einkäufe bei anderen Portalen berücksichtigt werden.

Neben den Rechten der Betroffenen ist auch ein etwaiges Bußgeld bei Verstößen gegen einzelne Vorgaben aus der DS-GVO nach Art. 83 DS-GVO nicht zu unterschätzen.

---

78 Albrecht/Jotzo, Teil 4, Rn. 27.

79 Wolff/Brink/Forgó, Art. 21, Rn. 28.

80 Sydow/Helfrich, Art. 21, Rn. 61.

81 Kühling/Buchner/Herbst, Art. 16, Rn. 9.

82 Vgl. auch Erwägungsgrund 71 UA 2 zum Profiling: „Um […] der betroffenen Person gegenüber eine faire und transparente Verarbeitung zu gewährleisten, sollte der für die Verarbeitung Verantwortliche geeignete mathematische und statistische Verfahren für das Profiling verwenden, […] mit denen in geeigneter Weise sichergestellt wird, dass Faktoren, die zu unrichtigen personenbezogenen Daten führen, korrigiert werden […]“.

83 Gola/Schulz, Art. 6, Rn. 131.

84 Plath/Kamlah, Art. 16, Rn. 10.

3. Zulässigkeit eines Scores als Grundlage für automatisierte Entscheidungen

Unabhängig von der Rechtmäßigkeit einer Verarbeitung schränkt Art. 22 DS-GVO die Möglichkeit ein, bedeutende Entscheidungen ausschließlich automatisiert zu treffen. Nach Art. 22 Abs. 1 DS-GVO sind Entscheidungen umfasst, die dem Betroffenen gegenüber rechtliche Wirkung entfalten oder ihn in ähnlicher Weise erheblich beeinträchtigen. Als Beispiele für eine solche Entscheidung nennt Erwägungsgrund 71[85] die automatische Ablehnung eines Online-Kreditantrags oder in einem Online-Einstellungsverfahren. Entgegen einer Ansicht[86] ist daher auch die Entscheidung über die Ablehnung eines Vertragsschlusses umfasst.[87]

Ein Social-Credit-System, das je nach (automatisiert ermitteltem) Punktestand Darlehen unter erleichterten Bedingungen vergibt oder die Gewährung anderer für den Nutzer bedeutsamer Leistungen daran knüpft, kann also dem Verbot des Art. 22 Abs. 1 DS-GVO unterfallen. Bei konsequenter weiter Auslegung des Art. 22 Abs. 1 DS-GVO, wie in der Literatur favorisiert,[88] ist sogar die (Nicht-)Gewährung von Leistungen wie Gutscheinen als erhebliche Beeinträchtigung umfasst. Angesichts der in den Erwägungsgründen genannten Beispiele und dem Erfordernis einer gerade erheblichen Beeinträchtigung, ist eine derart weite Auslegung ab-

---

85 Erwägungsgrund 71 UA 1: „Die betroffene Person sollte das Recht haben, keiner Entscheidung […] zur Bewertung von sie betreffenden persönlichen Aspekten unterworfen zu werden, die ausschließlich auf einer automatisierten Verarbeitung beruht und die rechtliche Wirkung für die betroffene Person entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt, wie die automatische Ablehnung eines Online-Kreditantrags oder Online-Einstellungsverfahren ohne jegliches menschliche Eingreifen. Zu einer derartigen Verarbeitung zählt auch das „Profiling", […] soweit dies rechtliche Wirkung für die betroffene Person entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt […]".

86 Gola/Schulz, Art. 22, Rn. 25.

87 Kühling/Buchner, Art. 22, Rn. 24; Sydow/Helfrich, Art. 22, Rn. 48; Paal/Pauly/Martini, Art. 22, Rn. 26.

88 Paal/Pauly/Martini, Art. 22, Rn. 48.

zulehnen. Erhebliche Auswirkungen sind jedoch insbesondere im Bereich Finanzen, Gesundheit und Arbeitsmarkt anzunehmen.[89] Bei deutlich erleichterter Darlehensgewährung, der Nutzung eines Hotels ohne Hinterlegung einer Sicherheit oder einer Kooperation mit Jobvermittlungsportalen greift Art. 22 Abs. 1 DS-GVO in der Regel.

Das Verbot gilt nicht, wenn die Entscheidung für den Abschluss oder die Erfüllung eines Vertrags erforderlich ist, aufgrund gesonderter Rechtsvorschriften zulässig ist[90] oder eine ausdrückliche Einwilligung des Betroffenen vorliegt, Art. 22 Abs. 2 DS-GVO. Soweit besondere Kategorien personenbezogener Daten – wie etwa politische Meinungen oder Gesundheitsdaten – in die Entscheidungsfindung einfließen, kommt für ein solches Social-Credit-System nach Art. 22 Abs. 4, Art. 9 Abs. 2 lit. a DS-GVO nur die Einwilligung in Betracht. Gegenüber Minderjährigen soll nach Erwägungsgrund 71 eine automatisierte Entscheidungsfindung nicht in Betracht kommen.[91]

Im Rahmen von Art. 22 Abs. 2 lit. a DS-GVO kann der jeweilige Vertragsinhalt zwischen Social Credit-Unternehmen und Nutzer erneut relevant werden. Soweit sich diesem nach Auslegung die Berechnung eines Scores zur Gewährung von Vorteilen als (Haupt-)Leistungspflicht entnehmen lässt, kann die automatisierte Entscheidung für die Vertragsdurchführung erforderlich sein. Nach Art. 22 Abs. 3 DS-GVO kann der Betroffene jedoch die Berücksichtigung seines Standpunktes und gegebenenfalls eine Neubewertung verlangen, sowie bei Vorliegen berechtigter Gründe auch das Eingreifen einer Person.[92]

Für das klassische Scoring hat der deutsche Gesetzgeber in § 31 BDSG 2018 eine Regelung geschaffen. Aus den Gesetzgebungsmaterialien ergibt sich nicht, auf welche Öffnungsklausel sich die Regelung stützen soll. Denkbar ist es, sie als Vorschrift im Sinne des Art. 22 Abs. 2 lit. b

---

89 Art. 29 Datenschutzgruppe, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, S. 22.

90 Siehe etwa § 37 BDSG 2018 für Entscheidungen im Rahmen der Erbringung einer Versicherungsleistung.

91 Vgl. Erwägungsgrund 71 UA 1: „[…] Diese Maßnahme sollte kein Kind betreffen."

92 Paal/Pauly/Martini, Art. 22, Rn. 39a-c.

DS-GVO[93] und Art. 6 Abs. 4 DS-GVO anzusehen.[94] Oder aber, sie mangels einschlägiger Öffnungsklausel aufgrund des Anwendungsvorrangs des Unionsrechts und der insoweit abschließenden DS-GVO überhaupt nicht zur Anwendung gelangen zu lassen.[95]

Auf die Anwendbarkeit des § 31 BDSG 2018 kommt es für ein Social-Credit-System nicht an. Anders als das klassische Scoring könnte ein Social-Credit-System einen Punktewert, z. B. 350-950, verwenden. Dieser ist jedoch nicht als Wahrscheinlichkeitswert im Sinne von § 31 Abs. 1 BDSG 2018 anzusehen. Der Punktewert soll die Zuverlässigkeit des Nutzers wiedergeben. Mit einem höheren Punktewert könnte auch die Wahrscheinlichkeit der Bonität und Zahlung steigen. Der Punktewert selbst enthält jedoch keine unmittelbare Aussage zu der Wahrscheinlichkeit. Er ist vielmehr eine Art Belohnungssystem mit Indizwirkung hinsichtlich der Bonität des Nutzers aus Sicht der Unternehmen. Der Sinn und Zweck, Schutz des Wirtschaftsverkehrs und Schutz des Kunden vor Überschuldung,[96] mit speziellen Regelungen hinsichtlich der Berücksichtigung nicht beglichener Forderungen und zu mathematisch-statistischen Verfahren passt gerade nicht auf einen einfachen Punktewert.

Schon aus diesem Grund kommt es für die Zulässigkeit der Berechnung des Scores letztlich erneut auf den jeweiligen Vertragsinhalt, Art. 22 Abs. 2 lit. a DS-GVO, bzw. eine Einwilligung des Betroffenen an, Art. 22 Abs. 2 lit. c DS-GVO. Dabei könnten gerade die genannten Rechte des Nutzers nach Art. 22 Abs. 3 DS-GVO in der Praxis ein Hindernis in Form von Mehraufwand darstellen – etwa wenn der Standpunkt des Nutzers Berücksichtigung finden soll.

---

93 Paal/Pauly/Frenzel, § 31, Rn. 1.

94 Taeger, ZRP 2016, S. 72, 74 f.

95 Kühling/Buchner, Art. 22, Rn. 4 f.

96 Vgl. BT-Drucks. 18/11325, S. 101: „Die […] Regelungen zu Auskunfteien und Scoring dienen dem Schutz des Wirtschaftsverkehrs und besitzen für Betroffene wie auch für die Wirtschaft eine überragende Bedeutung. Verbraucher vor Überschuldung zu schützen, liegt sowohl im Interesse der Verbraucher selbst als auch der Wirtschaft."

4. Zusammenfassende Betrachtung der Zulässigkeit eines (privaten) Social-Credit-Systems in Europa

Das europäische und deutsche Datenschutzrecht lassen nur wenig Spielraum für ein umfangreiches Social-Credit-System durch private Unternehmen.

Nur soweit ausschließlich juristische Personen betroffen sind und die Daten keine Rückschlüsse auf dahinterstehende natürliche Personen zulassen, fallen Verarbeitungsvorgänge nicht in den sachlichen Anwendungsbereich (vgl. Art. 4 Nr. 1 DS-GVO).

Im Übrigen ist für jeden Verarbeitungsvorgang ein Rechtfertigungstatbestand notwendig (Art. 6 DS-GVO). Ein Social-Credit-Unternehmen könnte dabei nur auf die Kooperation der Nutzer in Form einer freiwilligen Einwilligung oder eines Vertrags mit der Score-Berechnung als Leistungspflicht, am ehesten als Hauptleistungspflicht, setzen. Die Wahrung berechtigter Interessen scheidet bei einer derart umfassenden Zusammenführung von Daten unterschiedlichster Quellen aus. Nur bei der Zusammenführung innerhalb einer Unternehmensgruppe kann dieser Rechtfertigungsgrund in Betracht kommen. Soweit das Unternehmen gezielt Rückschlüsse z. B. zur politischen Meinung zieht und berücksichtigt, sind erhöhte Anforderungen zu stellen.

Die Betreiber des Social-Credit-Systems müssen zudem eine Datenschutz-Folgeabschätzung (Art. 35 DS-GVO) durchführen und einen Datenschutzbeauftragten benennen (Art. 37 DS-GVO, § 38 BDSG 2018).

Im Rahmen der Informationspflichten und des Auskunftsrechts der Betroffenen sind aussagekräftige Informationen über die Logik der Score-Berechnung mitzuteilen (Art. 13-15 DS-GVO). Den Betroffenen steht außerdem ein Anspruch auf Berichtigung zu, wenn sich der Score als unrichtig darstellt (Art. 16 S. 1 DS-GVO). Eine Vervollständigung durch Einbeziehung der Daten weiterer, anderer Onlineplattformen kann hingegen nicht verlangt werden (vgl. Art. 16 S. 2 DS-GVO). Soweit von dem Score erhebliche Auswirkungen, etwa als Grundlage einer Entscheidung über den Abschluss eines Darlehens, ausgehen, stehen dem Betroffenen weitergehende Rechte zu: insbesondere das Recht auf Einwirkung des Eingreifens einer Person seitens des Verantwortlichen, auf Darlegung des

eigenen Standpunktes und auf Anfechtung der Entscheidung (Art. 22 Abs. 3 DS-GVO).

Für Minderjährige ist eine automatisierte Entscheidungsfindung unzulässig (Erwägungsgrund 71 UA 1 a.E.) und im Übrigen kommt ein allgemeiner Rechtfertigungstatbestand zumindest für Kinder unter 16 Jahren ohne Mitwirkung der gesetzlichen Vertreter nicht in Betracht (vgl. Art. 6, 8 DS-GVO).

Die wirksame Einhaltung der genannten Rahmenbedingungen wird unter anderem durch hohe Bußgelder im Fall von Verstößen sichergestellt (Art. 83 DS-GVO).

VI. Fazit

Die Social-Credit-Testphase in China zeigt bereits eindrucksvoll, zu was Big Data imstande sein kann und imstande sein könnte. Der Score mit Datengrundlagen aus vielen Alltagssituationen soll das Vertrauen untereinander in der Gesellschaft fördern, kann aber auch als mächtiges Kontrollinstrument missbraucht werden. Schon jetzt deutet sich an, dass ein staatliches Social-Credit-System in China ab 2020 den Alltag der chinesischen Bürger entscheidend beeinflussen könnte.

In Europa und speziell in Deutschland ist ein derartiges staatliches System wohl schon aufgrund der politischen Kultur utopisch. Ein privates Social-Credit-System ist hinsichtlich natürlicher Personen nur bei einer entsprechenden Kooperationsbereitschaft der Personen realisierbar.

In absehbarer Zeit wird man sich in Europa also nicht (nur) über einen Score als bloße Zahl definieren. Es bleibt bei dem – insoweit frei interpretierten – Grundsatz des Philosophen René Descartes: „Ich denke, also bin ich."

Literaturnachweise

Albrecht/Jotzo, Das neue Datenschutzrecht der EU, Baden-Baden 2017.

Art. 29 Datenschutzgruppe, Guidelines on Consent under Regulation 2016/679, https://ec.europa.eu/newsroom/just/document.cfm?doc_id=48849 (zuletzt abgerufen: 11/2018).

Art. 29 Datenschutzgruppe, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, https://iapp.org/media/pdf/resource_center/W29-auto-decision_profiling_02-2018.pdf (zuletzt abgerufen: 11/2018).

Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht, 2. Auflage München 2016.

Ehmann/Selmayr, Datenschutz-Grundverordnung, München 2017.

Forgó/Helfrich/Schneider, Betrieblicher Datenschutz, 2. Auflage München 2017.

Gola, Datenschutz-Grundverordnung, München 2017.

Kühling/Buchner, Datenschutz-Grundverordnung, 2. Auflage München 2018.

Meissner, Chinas gesellschaftliches Bonitätssystem, https://www.merics.org/sites/default/files/2017-09/China%20Monitor_39_SOCS_DE.pdf (zuletzt abgerufen: 11/2018).

Paal/Pauly, Datenschutz-Grundverordnung/Bundesdatenschutzgesetz, 2. Auflage München 2018.

Plath, BDSG/DSGVO, 2. Auflage Köln 2016.

Schantz/Wolff, Das neue Datenschutzrecht, München 2017.

Sydow, Europäische Datenschutzgrundverordnung, Baden-Baden 2017.

Taeger, Scoring in Deutschland nach der EU-Datenschutzgrundverordnung, ZRP 2016, S. 72-75.

Wolff/Brink, Beck´scher Online-Kommentar Datenschutzrecht, 24. Edition 2018.

H. Big Data und die Versichertengemeinschaft – „Entsolidarisierung“ durch Digitalisierung? (Philip Bitter und Steffen Uphues)

Stand: November 2018

Abstract: Big Data und die Versichertengemeinschaft

Die Versicherungswirtschaft ist seit jeher auf Informationen über die Versicherten angewiesen. Das bietet ungeahnt viele Einsatzmöglichkeiten für Big Data. Mit Hilfe von Telematik, der Technologie zur Verhaltensdatenübermittlung, sollen Risiken entsprechend der Eigenschaften und Verhaltensweisen von Personen noch individueller eingeschätzt werden können und individuellere Prämien ermöglicht werden. Die Bedenken von Verbraucherschützern reichen insoweit bis hin zum möglichen Versicherungsverlust einiger Personengruppen. Schließlich könnte jeder Versicherte sein Risiko am Ende selbst tragen. Dabei werde das Solidarprinzip ausgehebelt. Das allgemeine Bedrohungsszenario einer „Entsolidarisierung“ der Versichertengemeinschaft ist jedoch unpräzise. Eine Differenzierung zwischen der Individualversicherung und der Sozialversicherung sowie zwischen den einzelnen Versicherungssparten erfolgt selten. Eine interdisziplinäre Betrachtung der Big-Data-basierten Tarif- und Prämienentwicklung in der Versicherung ist daher angezeigt.

I. Einleitung

Das Versicherungswesen war bisher nicht dafür bekannt, sehr innovativ und dynamisch zu sein. Nun ist die Branche im digitalen Zeitalter in Bewegung geraten und die Versicherer entdecken, auf einem Datenschatz sitzend, die Potentiale von Big Data in der Assekuranz.

Big Data – verstanden als Schlagwort für die Auswertung großer Datenmengen möglichst in Echtzeit – könnte einerseits dabei helfen, die sich

aus dem demografischen Wandel ergebenden Herausforderungen[1] in der Versicherung zu meistern und andererseits Wettbewerbsvorteile für Versicherungsunternehmen schaffen.[2]

Im Zuge der Digitalisierung erscheint eine stärkere Individualisierung von Tarifen und Prämien zulasten der Versichertengemeinschaft durch die zunehmende Datenerfassung und Datenauswertung möglich. Es wird daher auch von einer „Versicherungsrevolution“[3] gesprochen. Telematik-Tarife[4] und verhaltensbezogene Tarife sollen den Markt „revolutionieren“ [5]. Zudem heißt es, die Auseinandersetzung mit der Gefahr einer „schleichenden Entsolidarisierung“ von Versicherungen sei eine der „wesentlichen Herausforderungen“ von Big Data.[6] Danach sollen präzisere Risikoeinschätzungen zu einer Aufhebung der Versichertengemeinschaft als Solidargemeinschaft führen. Es liegt der als solidarisch empfundene Gedanke zugrunde, dass in einigen Versicherungen alle Versicherungsnehmer einen Versicherungsbeitrag zahlen, obwohl regelmäßig nur Einzelne von Schäden betroffen sind und die entsprechende Versicherungsleistung erhalten, während andere Versicherungsnehmer Beiträge zahlen ohne einen Schaden zu erleiden und die Leistung in Anspruch zu nehmen.

Nur ansatzweise werden dabei die verschiedenen Voraussetzungen und spezifischen Merkmale der Sozialversicherung und der Individualversicherung berücksichtigt. Vielmehr existiert in der gesellschaftlichen Wahr-

---

1 https://www.bundesgesundheitsministerium.de/themen/krankenversicherung/herausforderungen/demografischer-wandel.html (zuletzt abgerufen: 11/2018).

2 Vgl. Mayer-Schönberger/Cukier, S. 56/57.

3 http://www.faz.net/aktuell/wirtschaft/unternehmen/kommentar-die-versicherungs revolution-13704775.html (zuletzt abgerufen: 11/2018).

4 Dazu https://www.gdv.de/de/themen/news/wie-funktioniert-eigentlich-telematik--15500 (zuletzt abgerufen: 11/2018).

5 http://www.faz.net/aktuell/finanzen/meine-finanzen/versichern-und-schuetzen/nachrichten/versicherer-generali-belohnt-gesunden-lebensstil-mit-praemien-14308703.html (zuletzt abgerufen: 11/2018).

6 Maas/Milanova, Die Volkswirtschaft 05/2014, S. 23, 25.

nehmung oft ein allgemeines Bedrohungsszenario für das Versicherungswesen, in dem Big Data „das Solidaritätsprinzip“[7], „die Solidargemeinschaft“[8] oder „die Versichertengemeinschaft“[9] gefährde. Die gesellschaftliche Absicherung gegen Existenzrisiken wird schlussendlich in Frage gestellt.[10]

Wesentliche ökonomische, juristische oder soziologische Überlegungen geraten regelmäßig zu kurz. Wie stehen aber Kollektiv und Solidarität zueinander? Welche sind die Anwendungsbereiche von Big Data in der Branche? Schließlich ist die Diskussion um Chancen und Risiken individualisierter Tarife und Prämien nicht neu. Es ließe sich auch formulieren: Die der Branche vorgeworfene „Entsolidarisierung“ sei längst praktiziert.[11]

Durch den Einsatz von „Wearables“ in der Freizeit[12] und durch Telematik-Angebote von Versicherern steigt auch das Interesse der Bevölkerung an der Diskussion rund um die Versichertengemeinschaft und Big Data. Hierzu soll im Folgenden ein kurzer Überblick über den Status quo gegeben werden sowie über Auswirkungen von Big Data auf Versicherungsgrundsätze und das Szenario einer „Entsolidarisierung“.

II. Versicherung und Solidarität

Schon die Bestimmung der dafür zentralen Begriffe stellt eine Herausforderung dar. Der Versicherungsbegriff ist seit langer Zeit Gegenstand von Definitionsversuchen – auch weil sich der Gesetzgeber weitestgehend zurückhält. Bis heute fehlt es an einer allgemeingültigen Begriffserklä-

---

7 https://www.computerwoche.de/a/generali-vitality-durch-anreize-zum-glaesernen-versicherten,3312807 (zuletzt abgerufen: 11/2018).

8 http://digitalpresent.tagesspiegel.de/gesundheits-apps-das-ende-der-solidargemeinschaft (zuletzt abgerufen: 11/2018).

9 http://www.gdv.de/2015/11/droht-das-ende-der-versichertengemeinschaft/ (zuletzt abgerufen: 11/2018).

10 https://www.versicherungsbote.de/id/4851993/Versicherung-verlust-Versicherungsschutz/ (zuletzt abgerufen: 11/2018).

11 Erdmann/Schwarzbach, Zeitschrift für Versicherungswesen, S. 81, 82.

12 Vertiefend zum Thema Wearables: Delisle/Jülicher, in: Hoeren/Kolany-Raiser (Hrsg.), Big Data zwischen Kausalität und Korrelation, S. 95-107.

rung. Besondere Streitpunkte stellen sowohl die Frage nach der Abgrenzung der Sozial- und der Individualversicherung dar,[13] als auch die Einstufung der Sozialversicherung als Versicherung an sich.[14]

Eine **Versicherung** liegt zumindest nach Versicherungsvertragsrecht vor, wenn eine Partei sich gegen Entgelt verpflichtet, für den Fall eines ungewissen Ereignisses bestimmte Leistungen zu erbringen, wobei das übernommene Risiko auf eine Vielzahl durch die gleiche Gefahr bedrohter Personen verteilt wird und der Risikoübernahme eine auf dem Gesetz der großen Zahl beruhende Kalkulation zugrunde liegt.[15] Kurzum werden die Merkmale des privatwirtschaftlichen Versicherungsschutzes auch als „Deckung eines im Einzelnen ungewissen, insgesamt geschätzten Mittelbedarfs auf der Grundlage des Risikoausgleichs im Kollektiv und in der Zeit“ zusammengefasst.[16]

Daneben beschreibt das Bundesverfassungsgericht das Wesen der Sozialversicherung vor allem auch als die „gemeinsame Deckung eines möglichen, in seiner Gesamtheit schätzbaren Bedarfs durch Verteilung auf eine organisierte Vielheit.“[17]

Trotz dieser begrifflichen Annäherung bestehen zwischen Sozial- und Individualversicherung wesentliche Unterschiede. Die Auseinandersetzung damit kann dabei helfen, sich dem Szenario der Aushebelung des Solidarprinzips der Versicherung durch Big Data zu nähern.

1. Sozialversicherung

Im Gegensatz zur Individualversicherung ist die Sozialversicherung eine staatlich streng geregelte Pflichtversicherung.[18] Sie entsteht kraft oder zumindest aufgrund eines Gesetzes (vgl. § 31 Abs. 1 SGB I). Sie umfasst die im Sozialgesetzbuch normierte gesetzliche Renten-, Kranken-, Pflege-,

---

13 Beckmann/Matusche-Beckmann/Lorenz, § 1, Rn. 72.

14 Depenheuer, S. 68 ff.

15 Langheid/Wandt/Looschelders, § 1, Rn. 6.

16 Farny, S. 8.

17 BVerfG, Urteil vom 10.5.1960, BVerfGE 11, S. 105, 112 = NJW 1960, S. 1099 – Familienlastenausgleich.

18 Langheid/Wandt/Looschelders, § 1, Rn. 98.

Unfall- und Arbeitslosenversicherung und dient der sozialen Absicherung von Lebensrisiken.

Die selbstverwalteten Sozialversicherungsträger sind Körperschaften oder Anstalten des öffentlichen Rechts.[19] Als prägendes Merkmal – in Abgrenzung zur Individualversicherung – gilt das **Solidaritätsprinzip**[20], durch welches ein **sozialer Ausgleich** mit Umverteilungswirkung zwischen verschiedenen sozialen Gruppen vollzogen werden soll.[21]

2. Individualversicherung

Das Kerngeschäft in der Individualversicherung ist das **Risikogeschäft.**[22] Die Schadenverteilung wird dazu vom Versicherungsnehmer entgeltlich auf den Versicherer transferiert (Risikotransfer). Für die Risikoübernahme erhält der Versicherer eine Prämie.

Die Bestimmung der Risikoprämie orientiert sich an dem **versicherungstechnischen Äquivalenzprinzip** als Ausprägung des **Risikoprinzips**. Die Versicherungsbetriebswirtschaftslehre unterscheidet dabei zwischen dem kollektiven und dem individuellen Äquivalenzrisiko.[23]

Nach dem **kollektiven Äquivalenzprinzip** deckt die kollektive Risikoprämie mindestens den Erwartungswert des kollektiven Schadenbedarfs eines Versicherungsbestandes. Unter Schadenbedarf wird in der Versicherungspraxis dabei das arithmetische Mittel der Gesamtschäden einer homogenen Tarifklasse verstanden.[24]

Das **individuelle Äquivalenzprinzip** bestimmt die individuellen Risikoprämien nach dem individuellen Schadenbedarf – ermittelt auf der Grundlage verschiedener persönlicher Faktoren bei Abschluss des Versicherungsvertrags und nach dem gewünschten Leistungsspektrum.[25]

---

19 BVerfG, Urteil vom 10.5.1960, BVerfGE 11, S. 105, 112 = NJW 1960, S. 1099 – Familienlastenausgleich.

20 Depenheuer, S. 47.

21 Depenheuer, S. 53.

22 Farny, S. 22.

23 Farny, S. 67.

24 Albrecht, Zeitschrift für Versicherungswesen 2017, S. 157, 158.

25 Farny, S. 68.

Um ausreichend einzelne Prämien zur Deckung aller Schadenfälle kalkulieren zu können, muss das Versicherungsunternehmen unter anderem den gesamten Schadenbedarf eines Kollektivs in Geld schätzen.[26] Außerdem bedarf es statistischer Grundlagen zur persönlichen Schadenerwartung, die in der Regel aus Erfahrungswerten gewonnen werden.

Hier setzt Big Data an und ermöglicht die Einbeziehung von unstrukturierten Daten sowie von Daten aus unterschiedlichen Quellen und somit eine weitere Annäherung an das individuelle Risiko. Da sich ein einzelnes Risiko aber aufgrund des Zufallsfaktors bei dem Eintritt von Schäden schwer schätzen lässt, ist immer noch eine statistische Masse notwendig, aus der valide Durchschnittswerte ermittelt werden können. Die private Versicherungswirtschaft richtet sich nach dem wahrscheinlichkeitstheoretischen **„Gesetz der großen Zahl“**: Je mehr zugrundeliegende Einzelwerte vorliegen, desto zuverlässiger sind die Durchschnittswerte.[27]

Aber auch in der Individualversicherung sind in bestimmten Rechnungsperioden nur einzelne Versicherte von Schäden betroffen und nehmen den Ausgleich in Anspruch, während andere schadenfrei bleiben. Für das Einzelrisiko entstehen individuelle „Überschäden“ und „Unterschäden“, indem der Effektivwert der Schäden den Erwartungswert über- oder unterschreitet.[28] Bei der Individualversicherung findet daher schließlich ebenso ein Ausgleich statt. Genauer betrachtet handelt es sich jedoch um einen Ausgleich zufälliger Schwankungen im Schadenverlauf sowie in der Zeit und nicht um den Ausgleich systematischer Unterschiede in der Schwere der individuellen Risiken.[29]

Somit greift die Individualversicherung zwar den Gedanken der kollektiven Übernahme des Risikos als Versicherungsprinzip auf und der Ausgleich im Kollektiv wird zum Teil als „solidarisch“ bezeichnet. Solidaritätsprinzip und sozialer Ausgleich als Formen der Solidarität werden

---

26 Müller-Peters/Wagner, S. 4.

27 Müller-Peters/Wagner, S. 4.

28 Farny, S. 46.

29 Depenheuer, S. 54; Albrecht, Zeitschrift für Versicherungswesen 2017, S. 157, 158.

aber weit überwiegend der Sozialversicherung zugewiesen.[30] Die Versichertengemeinschaft in der Individualversicherung ist dann nicht als Solidargemeinschaft konstituiert, sie beruht nicht auf dem Solidaritätsprinzip der Sozialversicherung.

3. „Entsolidarisierung“?

Eine undifferenzierte Verwendung der Begriffe der Solidargemeinschaft und des Solidaritätsprinzips führt zu einer Vermischung mit dem versicherungstechnischen Prinzip des Ausgleichs von Risiken im Kollektiv.[31] Bei der Personalisierung von Prämien und Tarifen durch Big Data in der Individualversicherung wird auch von einer „Fragmentierung“ der Versicherungskollektive gesprochen.[32] Die Argumentation einer möglichen „Entsolidarisierung“ ohne Abgrenzung von Sozial- und Individualversicherung ist dagegen zwar eingängig, wird aber als terminologisch unscharf eingeordnet.[33]

III. Anwendungen von Big Data

Gemessen an der Datenmenge besitzt das Versicherungswesen ein großes digitales Potential. Es bieten sich vielfältige Anknüpfungspunkte für den Einsatz von Big-Data-Technologie. Neben der unternehmensinternen Anwendung – etwa im automatisierten Schadenmanagement – bietet sich Big Data besonders zur Tarifgestaltung an.

Es können immer mehr Daten erfasst werden. Darunter finden sich individuelle Verhaltens- und Gesundheitsdaten der Versicherten, die bislang kaum verfügbar waren. Außerdem ermöglichen neue Analyseverfahren die Verknüpfung bislang unstrukturierter Daten und deren Auswertung.

Mit **Telematik**-Tarifen wird dabei vorwiegend die Kfz-Versicherung in Verbindung gebracht. Obwohl die Anzahl der Telematik-Tarife auch in der Kfz-Versicherung noch gering ist, gibt es kaum größere Versicherer,

---

30 Erdmann/Schwarzbach, Zeitschrift für Versicherungswesen, S. 81, 83.

31 Müller-Peters/Wagner, S. 14.

32 Looschelders, Zeitschrift für die gesamte Versicherungswirtschaft 2015, S. 481 ff.

33 Albrecht, Zeitschrift für Versicherungswesen 2017, S. 157, 158.

die sich mit Telematik nicht beschäftigen.[34] Die Berechnung der Prämie in der Kfz-Versicherung ist komplex. Verschiedene Faktoren, wie zum Beispiel Fahrzeugtyp, Zulassungsort und Unfallfreiheit, spielen eine Rolle. Anhand von Statistiken werden daher unterschiedliche Punkte, z. B. die Unfallhäufigkeit in der Region oder die Anzahl der verschiedenen Fahrer berücksichtigt, obwohl häufig doch stärker der individuelle Fahrstil über das Unfallrisiko entscheidet. Aus diesem Grund werden Tarife, die das individuelle Fahrverhalten betreffen, auch häufig als gerecht empfunden.[35]

Telematik-Tarife sollen den individuellen Verhaltensfaktor nun stärker berücksichtigen. Technisch umgesetzt werden entsprechende Angebote durch eine Telematik-Box oder eine App auf dem Smartphone. Das Fahrverhalten wird so während der Autofahrt überwacht, sämtliche Daten werden erfasst und zu einem „Score“ zusammengezogen. Umsichtiges Fahren, welches sich in dem „Score“ widerspiegelt, wird schließlich mit Rabatten belohnt.

Die Score-Kriterien sind von Versicherung zu Versicherung zwar unterschiedlich, regelmäßig sind jedoch Geschwindigkeit, Beschleunigung sowie Brems- und Kurvenverhalten die wesentlichen Indikatoren.[36]

Zielgruppe von Telematik-Tarifen sind dabei vor allem junge Fahrer, die aufgrund der geringen Fahrpraxis in der Regel mit sehr hohen Prämien starten. So bieten auf dem deutschen Kfz-Versicherungsmarkt einige Versicherungsmarken bereits solche „Pay As You Drive“-Tarife an. Ein Großteil der Versicherer hält sich mit der Einführung aber noch zurück.

„Pay As You Live“-, „Self Tracking“- oder „Vitalitäts-Tarife“ sollen bei gesundheitsbewusstem Verhalten, nachgewiesen etwa durch eine Datenübermittlung von Wearables, für eine Beitragsentlastung sorgen. Zu finden sind derartige Programme zum Beispiel bei der Generali in der Berufsunfähigkeits- und Lebensversicherung. Darüber soll sich gesundheitsbewusstes Verhalten auf die Überschussbeteiligung auswirken.

---

34 Erdmann/Schwarzbach, Zeitschrift für Versicherungswesen, S. 81.

35 Müller-Peters/Wagner, S. 29 ff.; O´Neil, S. 165 ff.

36 http://positionen.gdv.de/guenstige-tarife-dank-telematik/ (zuletzt abgerufen: 11/2018)

IV. Ökonomische Implikationen

Der Gedanke einer Differenzierung zwischen „Entsolidarisierung“ und „Fragmentierung“ der Versicherungskollektive lässt sich durch wirtschaftliche Überlegungen festigen: Die Prämiendifferenzierung als Folge des Äquivalenzprinzips führt betriebswirtschaftlich zu einer Unabhängigkeit der einzelnen Prämien von der Zusammensetzung des kollektiven Versicherungsbestandes. Die differenzierten Risikoprämien ergeben unabhängig von der Ausgestaltung des Kollektivs den kollektiven Schadenerwartungswert.[37]

Undifferenzierte Prämien können in der privaten Versicherungswirtschaft dagegen die Gefahr einer „adversen Selektion“ mit sich bringen.[38] Bedingt auch durch die im Rahmen von Art. 2 Abs. 1 GG gewährleistete Vertragsfreiheit als Ausprägung der Privatautonomie im Zivilrecht und die gleichzeitige Informationsasymmetrie der Vertragspartner bei Vertragsschluss, kommt es in diesem Szenario vermehrt zu Auswechslungen im Versichertenkollektiv und letztendlich zu einer Negativauslese.[39] Zahlen Versicherungsnehmer mit unterdurchschnittlicher Schadenerwartung die gleichen Prämien wie Versicherungsnehmer mit überdurchschnittlicher Schadenerwartung, versichern sie sich nicht mehr oder es zieht sie zu konkurrierenden Versicherungsunternehmen mit risikogerechteren Prämien. Versicherungsnehmer mit überdurchschnittlicher Schadenerwartung und daher für sie „günstigeren“ Prämien treten dagegen neu in das Kollektiv ein.

Im Beispiel der privaten Krankenversicherung besteht die Versichertengemeinschaft dann etwa nur noch aus kranken und alten Kunden und das Unternehmen kann die Kosten für die Versicherung nicht mehr tragen.[40] Die risikogerechte Prämiendifferenzierung ist danach sogar ein betriebswirtschaftlicher Grundsatz der Individualversicherung.[41]

---

37 Farny, S. 70.

38 Albrecht, Zeitschrift für Versicherungswesen 2017, S. 157, 158.

39 Müller-Peters/Wagner, S. 8.

40 Albrecht, Zeitschrift für Versicherungswesen 2017, S. 157, 158.

41 Farny, S. 70.

Zusätzlich sieht sich ein privates Versicherungsverhältnis bei nachvertraglichen Informationsasymmetrien dem moralischen Risiko einer risikogeneigten Verhaltensänderung des Versicherten durch die Versicherung („moral hazard“) ausgesetzt. Auch diesem Effekt soll eine risikogerechte Differenzierung entgegenwirken.[42]

Die Individualversicherung besitzt vielmehr auch bei individuellen Tarifen und Prämien einen kollektiven Charakter.[43] Denn der Schadenerwartungswert eines Versicherungsvertrags kann nicht allein durch individuelle Daten des Versicherungsnehmers ermittelt werden. Der Schadeneintritt ist nie ganz vorhersehbar und muss somit immer geschätzt werden. Eine individuell risikogerechte Tarifierung ist damit stets auch abhängig vom Kollektiv und die gebildeten Tarifklassen werden mit den Schadenerfahrungen aus anderen Klassen und dem Gesamtkollektiv verknüpft.[44]

Die Unterscheidung von Kollektiven würde vom freien Markt demnach erzwungen.[45] Man könnte auch sagen: „Die selbst verordnete und beherrschende Handlungsformel, Risiko gleich Prämie nach dem Äquivalenzprinzip, beinhaltet schon in ihrem Ansinnen und der logischen Zielsetzung die Negierung von Gleichbehandlung und Solidarität“.[46]

V. Rechtliche Rahmenbedingungen

Aus juristischer Perspektive ist zu klären, inwieweit einfachgesetzliche und verfassungsrechtliche Vorgaben bestehen, die es bei der Entwicklung Big-Data-basierter, individueller Tarife zu berücksichtigen gilt. Es ist wiederum zwischen der Sozialversicherung und der Individualversicherung zu unterscheiden. Für beide Bereiche besteht ein Regelungsgeflecht, in das Big-Data-getriebene Versicherungsangebote einzuordnen sind. Das gilt besonders für das Aufsichts- und das Vertragsrecht. Hinzu

---

42 Swedloff, Conneticut Insurance Law Journal 21.1/2014, S. 339, 346.

43 Albrecht, Zeitschrift für Versicherungswesen 2017, S. 189 ff.

44 Albrecht, Zeitschrift für Versicherungswesen 2017, S. 189 ff.

45 Butzer, S. 205.

46 So Erdmann/Schwarzbach, Zeitschrift für Versicherungswesen, S. 81, 83.

kommen datenschutzrechtliche Vorgaben, die im Rahmen der Solidaritätsdiskussion jedoch nur am Rande in Erscheinung treten.[47]

1. Individualversicherung

Bei der Individualversicherung entsteht das Versicherungsverhältnis durch den Abschluss eines privatrechtlichen Versicherungsvertrags zwischen dem Versicherungsunternehmen und dem Versicherungsnehmer.[48] In diesem Zuge können die Leistungen und Gegenleistungen im Sinne der Privatautonomie grundsätzlich frei zwischen den Vertragsparteien ausgehandelt werden.

Zu berücksichtigen sind dabei vor allem einfachgesetzliche Vorschriften, insbesondere Regelungen des Versicherungsvertragsgesetzes (VVG). Im Bereich der Kfz-Versicherung[49], aber auch bei der Lebens- und Berufsunfähigkeitsversicherung[50], wird vor allem das Verhältnis zu den Gefahrerhöhungsvorschriften der §§ 23 ff. VVG diskutiert.

Nach §§ 153 Abs. 2 S. 1, 176 VVG gilt für die Lebens- und Berufsunfähigkeitsversicherung, dass der Versicherer die Beteiligung am Überschuss nach einem verursachungsorientierten Verfahren durchführen muss. So wird es als „grundsätzlich vertretbar“ eingeordnet, gesundheitsbewusstes Verhalten, welches das Risiko beeinflusst und zur Entstehung von Überschüssen beiträgt – im Einklang mit dem Gleichbehandlungsgebot und versicherungstechnisch nachvollziehbar begründet – im Rahmen einer Überschussverteilung zu berücksichtigen.[51]

Ferner müssen für von Rechtsvorschriften abweichende oder diese ergänzende Regelungen die §§ 307 ff. BGB zu Allgemeinen Geschäftsbedingungen (AGB) eingehalten werden.[52]

Für die private Krankenversicherung etwa antwortete die Bundesregierung auf eine Kleine Anfrage der Fraktion DIE LINKE u. a. im Deutschen

---

47 Vgl. dazu: Rubin, recht + schaden 2018, S. 337, 343 ff.

48 Langheid/Wandt/Looschelders, § 1, Rn. 96.

49 Klimke, recht + schaden 2015, S. 217 ff.

50 Brömmelmeyer, recht + schaden 2017, S. 225, 229.

51 Brömmelmeyer, recht + schaden 2017, S. 225, 228.

52 Brömmelmeyer, recht + schaden 2017, S. 225, 230 f.

Bundestag auch, dass § 203 VVG abschließend regele, „unter welchen Voraussetzungen die Beiträge […] erhöht werden können“ und dass „eine Weigerung [des Versicherten], an erweiterten Datensammlungen bezüglich seiner Gesundheit und seines Lebenswandels teilzunehmen“, die Voraussetzungen des § 203 VVG dabei nicht erfülle.[53]

Schließlich stellt auch das Versicherungsaufsichtsrecht Anforderungen. So heißt es für die Lebensversicherung und die private Krankenversicherung in §§ 138 Abs. 2, 146 Abs. 2 Satz 1 VAG: „Bei gleichen Voraussetzungen dürfen Prämien und Leistungen nur nach gleichen Grundsätzen bemessen werden.“ Damit soll eine Diskriminierung auch im Rahmen der Überschussbeteiligung verhindert und eine verhaltensberücksichtigende Differenzierung auf rationale Kriterien gestützt werden.[54] Beitragsermäßigungen dürfen letztlich nicht zulasten anderer Tarife gehen.[55]

Im Umkehrschluss könnte man daraus auch entnehmen, dass die Mitgliedsbeiträge bei ungleichen Voraussetzungen anzupassen seien und somit eine Ausrichtung anhand der individuellen Beschaffenheit des Versicherungsnehmers – also eine risikogerechte Prämiendifferenzierung – aufsichtsrechtlich gerade gefordert ist.[56]

Gesondert zu betrachten ist die private Krankenversicherung ferner deshalb, weil sie speziell dazu angelegt ist, den Sozialversicherungsschutz im dualen Krankenversicherungssystem zu ersetzen, vgl. § 146 VAG, § 195 VVG. Mit Art. 44 des GKV-WSG (Gesetz zur Stärkung des Wettbewerbs in der gesetzlichen Krankenversicherung) wurde 2009 der Basistarif eingeführt. Seither müssen die Vertragsleistungen privater Versicherungen im Basistarif mit den Pflichtleistungen der gesetzlichen Krankenversicherung vergleichbar sein, § 152 Abs. 1 VAG.

Darüber hinaus legt die Krankenversicherungsaufsichtsverordnung zur Prämienkalkulation in § 10 KVAV fest, dass die Berechnung für jede Per-

---

53 BT-Drucksache 18/3849 vom 28.01.2015, S. 5, online verfügbar unter: http://dipbt.bundestag.de/doc/btd/18/038/1803849.pdf (zuletzt abgerufen: 11/2018).

54 Brömmelmeyer, recht + schaden 2017, S. 225, 227.

55 Brömmelmeyer, recht + schaden 2017, S. 225, 228.

56 Albrecht, Zeitschrift für Versicherungswesen 2017, S. 157, 159.

son altersabhängig getrennt für jeden Tarif und anhand einer nach Einzelaltern erstellten Prämienstaffel zu erfolgen hat. Weitere Differenzierungsmerkmale sind nicht vorgesehen. Eine unmittelbare verhaltensabhängige Kalkulation wird, im Gegensatz zu derzeitigen Bonusprogrammen, mit den Rechnungsgrundlagen der KVAV als unvereinbar eingestuft.[57]

Zwar sind einige rechtliche Fragen zur Umsetzung von Big-Data-basierten Tarifen mit laufender Datenerfassung und -auswertung in der Individualversicherung erst in Ansätzen geklärt. Dennoch ist für die „Fragmentierung" von Versicherungskollektiven in der Individualversicherung zu beachten, dass speziell für das Beispiel der privaten Krankenversicherung, rechtliche Vorgaben zum Schutz vor „ungerechten" oder „unsozialen" Prämien schon bestehen.[58] So gilt es auch diese in der Diskussion zu berücksichtigen.

2. Sozialversicherung

Nach der Kompetenzzuweisung des Art. 74 Abs. 1 Nr. 12 GG steht dem Bund auf dem Gebiet der Sozialversicherung die konkurrierende Gesetzgebung zu. Das Sozialversicherungsrecht ist dabei eines der wichtigsten Instrumente staatlicher Sozialpolitik und der Schutz etwa in Fällen von Krankheit in der sozialstaatlichen Ordnung des Grundgesetzes eine Grundaufgabe des Staates.[59] Das in Art. 20 Abs. 1 GG verankerte Sozialstaatsprinzip trägt dem Gedanken Rechnung, dass das rechtsstaatliche Versprechen von Freiheit erst durch eine Existenzabsicherung in ein reales Freiheitsgefühl umgesetzt werden kann.[60]

Die vorhandenen gesetzlichen Regelungen bilden dabei einen vergleichsweise strengen Rechtsrahmen, der eine Individualisierung von Sozialversicherungsleistungen nur in Grenzen zulässt.

---

57 Brömmelmeyer, recht + schaden 2017, S. 225, 228.

58 Albrecht, Zeitschrift für Versicherungswesen 2017, S. 157, 159.

59 BVerfG, Beschluss vom 6.12.2005, BVerfGE 115, S. 25, 43 = NJW 2006, S. 891, 892 – Bioresonanztherapie.

60 Michael/Morlok, § 7, Rn. 3.

Bei Vorliegen bestimmter Umstände besteht für den Einzelnen etwa eine Versicherungspflicht, vgl. insb. § 5 SGB V, §§ 1 ff. SGB VI, §§ 2, 3 SGB VII. Durch diese Pflicht soll verhindert werden, dass eine Auslese zum Beispiel nach Gesundheitsrisiken erfolgt.

Die Krankenkassen dürfen personenbezogene Daten ihrer Mitglieder auch nur in ausdrücklich geregelten Ausnahmefällen erheben und speichern, § 284 SGB V.

Bewegungsdaten von Tracking-Apps, die zu Bonusleistungen führen sollen, genügen nach Auffassung des Bundesversicherungsamts als Aufsichtsbehörde für die Sozialversicherungen zudem nicht den Anforderungen des § 65a Abs. 1 SGB V hinsichtlich „Nachweisbarkeit“ und „Qualitätssicherung“ der Bewegungsdaten.[61]

VI. Soziologische Implikationen

Aus soziologischer Perspektive wird eine Rückbesinnung zur Solidarität zum Teil auch für die Individualversicherung gefordert. „Ein Abgleich zwischen geschäftlicher Notwendigkeit und gesamtgesellschaftlicher Funktionalität“ sei „dringend erforderlich“.[62]

Es sei „unerlässlich, dass für eine Selbstverständnisdiskussion der Branche andere wissenschaftliche Disziplinen herangezogen werden.“[63] Auch die simple Umverteilung von Geldmitteln in Schadenfällen sollte so „nicht allein betriebswirtschaftlichen und juristischen Kalkülen unterliegen.“[64] Die „Existenzhilfe“ sei als „wesentlicher Bestandteil des Versicherungsgedankens“ zu sehen und Schäden und Unglücksfälle immer Bestandteile eines „sozialen Milieus“. Die Versicherung könnte damit als „gesellschaftliche Praxis der Verantwortung zur Bewältigung von Sicherheitsbedürfnissen“ betrachtet werden.[65]

---

61 Bundesversicherungsamt im Tätigkeitsbericht 2016, S. 25: http://www.bundesversicherungsamt.de/fileadmin/redaktion/Presse/epaper2016/index.html#25 (zuletzt abgerufen: 11/2018).

62 Erdmann/Schwarzbach, Zeitschrift für Versicherungswesen, S. 162, 164.

63 Erdmann/Schwarzbach, Zeitschrift für Versicherungswesen, S. 162, 163.

64 Erdmann/Schwarzbach, Zeitschrift für Versicherungswesen, S. 162, 162.

65 Erdmann/Schwarzbach, Zeitschrift für Versicherungswesen, S. 162, 163.

IV. Fazit

Der Solidaritätsbegriff wird im Zusammenhang mit dem digitalen Strukturwandel in der Versicherungslandschaft uneinheitlich verwendet. Das Verhältnis von Versicherung und Solidarität ist umstritten: Die Diskussion der Solidarität in der Sozialversicherung und darüber, ob und in welcher Form sie auch ein Element der Individualversicherung darstellt, gerät dabei zu kurz.

Eine interdisziplinäre Begleitung der Entwicklung entsprechender Tarife auf Verhaltensbasis ist angezeigt. Auf die Unterschiede zwischen Individualversicherung und Sozialversicherung ist dabei hinzuweisen. Das Szenario der „Entsolidarisierung“ durch Big Data in der Versicherung muss sich vor allem an juristischen, ökonomischen und soziologischen Kriterien messen lassen.

Literaturnachweise

Albrecht, Bedroht Big Data Grundprinzipien der Versicherung?, Zeitschrift für Versicherungswesen 2017, S. 157 – 161.

Albrecht, Bedroht Big Data Grundprinzipien der Versicherung? (II.), Zeitschrift für Versicherungswesen 2017, S. 189 – 192.

Brömmelmeyer, Belohnungen für gesundheitsbewusstes Verhalten in der Lebens- und Berufsunfähigkeitsversicherung? Rechtliche Rahmenbedingungen für Vitalitäts-Tarife, recht + schaden 2017, S. 225 – 232.

Butzer, Fremdlasten in der Sozialversicherung – Zugleich ein Beitrag zu den verfassungsrechtlichen Vorgaben für die Sozialversicherung, Tübingen 2001.

Depenheuer, Solidarität im Verfassungsstaat: Grundlegung einer normativen Theorie der Verteilung, 2. Auflage Norderstedt 2016.

Delisle/Jülicher, Step Into The Circle – Wearables und Selbstvermessung im Fokus, in: Hoeren/Kolany-Raiser (Hrsg.), Big Data zwischen Kausalität und Korrelation, S. 95-107, Münster 2016.

Erdmann/Schwarzbach, Telematiktarife und der Ruf nach Solidarität, Ein (Rück-)Besinnungsaufsatz (I.), Zeitschrift für Versicherungswesen 2017, S. 81 – 83.

Erdmann/Schwarzbach, Telematiktarife und der Ruf nach Solidarität, Ein (Rück-)Besinnungsaufsatz (III.), Zeitschrift für Versicherungswesen 2017, S. 162 – 164.

Farny, Versicherungsbetriebslehre. 5. Auflage Karlsruhe 2011.

Klimke, Telematik-Tarife in der Kfz-Versicherung, recht + schaden 2015, S. 217 – 268.

Langheid/Wandt, Münchener Kommentar zum VVG, Band 1, 2. Auflage München 2016.

Looschelders, Fragmentierung der Kollektive in der Privatversicherung – juristische Implikationen, Zeitschrift für die gesamte Versicherungswissenschaft 2015, S. 481 – 499.

Beckmann/Matusche-Beckmann, Versicherungsrechts-Handbuch, 1. Teil, 1. Abschnitt, 3. Auflage München 2015.

Maas/Milanova, Zwischen Verheißung und Bedrohung: Big Data in der Versicherungswirtschaft, Die Volkswirtschaft 05/2014, S. 23 – 25, http://die volkswirtschaft.ch/content/uploads/2014/05/11_Maas_Milanova_ DE.pdf (zuletzt abgerufen: 11/2018)

Mayer-Schönberger, Cukier, Big Data – A Revolution That Will Transform How We Live, Work, and Think, New York 2014.

Michael/Morlok, Staatsorganisationsrecht, 2. Auflage Baden-Baden 2015.

Müller-Peters/Wagner, Geschäft oder Gewissen? Vom Auszug der Versicherung aus der Solidargemeinschaft, 2017, http://goslar institut.de/ fileadmin/fuerAdmin/bilder/Broschueren/2017/_GESCHA%CC%88FT_ ODER_GEWISSEN_BROSCHUERE_05.04.17_15.25_.pdf (zuletzt abgerufen: 11/2018).

O'Neil, Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy, New York 2016.

Rubin, Inhalt und versicherungsrechtliche Auswirkungen der Datenschutz-Grundverordnung, recht + schaden 2018, S. 337 – 345.

Swedloff, Risk Classification's Big Data (R)evolution, Conneticut Insurance Law Journal Vol. 21.1 2014, S. 339 – 373.

I. Big-Data-Überwachung am Arbeitsplatz – Grenzen der Zulässigkeit durch aktuelle Gerichtsentscheidungen (Nicolai Culik und Lukas Forte)

Stand: Oktober 2017

Abstract: Überwachung am Arbeitsplatz

Big Data findet im Personalwesen vermehrt Anwendung, etwa zu Zwecken der Bewerberauswahl oder der Optimierung von Arbeitsabläufen. Das Datenschutzrecht zieht für die Erhebung und Verarbeitung von Beschäftigtendaten allerdings Grenzen, die kürzlich vom Bundesarbeitsgericht und dem Europäischen Gerichtshof für Menschenrechte gestärkt wurden. Keylogger beispielsweise dürfen zur Überwachung der Arbeitnehmer nicht heimlich eingesetzt werden. Dies gilt auch bei Verdacht der übermäßig privaten Nutzung des Dienst-PCs, sodass Kündigungen, die sich auf derart gewonnene Informationen stützen, unwirksam sind. Vielmehr muss für die heimliche Informationsbeschaffung ohne Einwilligung des Betroffenen ein konkreter Verdacht einer schweren Pflichtverletzung oder einer Straftat vorliegen; ansonsten sind Einwilligungen einzuholen oder Betriebsvereinbarungen abzuschließen. Diese Anforderungen an die Überwachung von Arbeitnehmern sind höher als etwa in den USA und haben auch zukünftig trotz europäischer und nationaler Änderungen im Datenschutzrecht Bestand.

I. Einleitung

Für Big Data, also die schnelle Verarbeitung umfangreicher und unterschiedlicher Datenbestände, gibt es auch im Arbeitsverhältnis Anwendungsbedarf. Der Nutzen liegt nämlich grundsätzlich darin, aus der Vergangenheit Schlüsse zu ziehen, um bestmögliche Entscheidungen für die

Zukunft zu treffen. Durch die kombinierte und systematische Analyse allerhand Randparameter werden bestimmte Abhängigkeiten und Muster erkannt, die im jeweiligen Zusammenhang genaue Prognosen zulassen.

1. Big Data im Personalwesen

Auch Personalentscheidungen sind das Ergebnis eines Analyse-Prozesses und stellen eine Prognose dar. In einem Bewerbungsgespräch wird versucht, sich ein Bild davon zu machen, wie erfolgreich der Bewerber später arbeiten wird und welchen Nutzen er dem Unternehmen voraussichtlich einbringt. In diesem Zusammenhang gibt es Ansätze, sich weniger auf das eigene Bauchgefühl, als auf errechnete Korrelationen zu verlassen. Zeigt sich beispielsweise, dass besonders erfolgreiche Mitarbeiter bestimmte Charaktereigenschaften aufweisen oder spezielle Qualifikationen mitbringen, könnte es Sinn ergeben, diese Merkmale bei der Bewerberauswahl stärker zu gewichten. Die Ermittlung der Daten muss dafür nicht länger allein klassisch durch Bewerbungsunterlagen und Gespräche erfolgen. Durchgeführt werden können z. B. auch Online-Background-Checks, etwa durch das automatisierte Abfragen sozialer Netzwerke.

Doch nicht nur zur Bewerberauswahl können Big-Data-Anwendungen im Personalwesen eingesetzt werden. Schließlich erfolgt ein Großteil der Auswahlentscheidungen in Unternehmen im Zuge der Beförderung oder Versetzung von Mitarbeitern oder bei der Zusammenstellung von Projektteams. Weitere Zwecke der Analyse können Laufbahnplanung, Teamentwicklung, Trainingsbedarfsanalyse, Standortbestimmung oder Potentialanalyse sein. Auch dafür ist es von großem Nutzen, Leistungsdaten des betroffenen Arbeitnehmers zu messen und in die Entscheidung einfließen zu lassen. In seinem erst kürzlich ergangenen Urteil zog das Bundesarbeitsgericht Grenzen der rechtlichen Zulässigkeit.[1] Speziell ging es dabei um den Einsatz von Keyloggern.

---

1 BAG, Urteil vom 27.07.2017 – 2 AZR 681/16.

2. Was ist Keylogging?

Keylogger (dt. „Tasten-Protokollierer“) erfassen sämtliche Tastenanschläge und Eingaben des PC-Nutzers und senden diese in regelmäßigen Abständen an den eingestellten Empfänger. So ist es möglich, Screenshots von allen auf dem Bildschirm des PC-Nutzers verfolgten Aktivitäten zu übermitteln und sogar die Webcam unerkennbar zu öffnen und Bilder des PC-Nutzers aufzunehmen.[2]

Zwei Arten von Keyloggern können unterschieden werden: Hardwarebasierte Keylogger erfordern eine unmittelbare physische, z. B. drahtgebundene, Verbindung zum Betriebssystem und schalten sich zwischen Tastatur und Rechner. Die erlangten Daten werden dabei in einem integrierten Speicher gesammelt. Bei den softwarebasierten bzw. drahtlosen Keyloggern werden die Tastenanschläge stattdessen regelmäßig unverschlüsselt per Funkübertragung an den PC versandt, sodass ein Angreifer die Daten ohne größeren Aufwand abfangen und die getätigten Eingaben rekonstruieren kann.[3] Im vor dem Bundesarbeitsgericht verhandelten Fall setzte der Arbeitgeber einen solchen softwarebasierten Keylogger ein. Diese Keylogging-Technik wird meist von Hackern als Virus oder Trojaner installiert, um Unternehmensdaten auszuspähen oder vertrauliche Daten der Nutzer, wie Kennwörter, PINs, Kreditkartennummern und Zugänge zu Benutzeraccounts, abzufangen.[4]

II. Aktuelles Urteil des Bundesarbeitsgerichts

Im Fokus stand bei dem Gerichtsverfahren die Frage, ob die aus dem heimlichen Einsatz eines Keyloggers zur Aufzeichnung der Aktivitäten des Arbeitnehmers gewonnen Daten für eine Kündigung verwendet werden dürfen.

---

2 Ciampa, S. 85.

3 Vogelsang et al., DuD 2016, S. 729, 730.

4 Gabler Wirtschaftslexikon.

1. Sachverhalt der Entscheidung

In dem Verfahren vor dem Bundesarbeitsgericht wehrte sich ein Web-Entwickler gegen die Kündigung seiner Agentur. Diese hatte der Belegschaft im Zusammenhang mit der Freigabe eines neuen WLAN-Netzwerks mitgeteilt, dass nunmehr sämtliches Datenaufkommen (sog. Traffic) aufgezeichnet und dauerhaft gespeichert werde, um rechtlichem Missbrauch vorzubeugen, bzw. um diesen aufzuklären. Zu diesem Zweck wurde auf dem Dienst-PC des Arbeitnehmers auch heimlich ein Keylogger installiert, der dessen Surf-Verhalten protokollierte und speicherte.

Durch Auswertung der Log-Dateien gelang es der Agentur, herauszufinden, dass der Arbeitnehmer das Internet und seine Arbeitszeit in erheblichem Umfang für private Zwecke nutzte, z. B. die Programmierung eines Computerspiels oder die Verwaltung von Aufträgen aus dem Unternehmen seines Vaters. Daraufhin kündigte der Arbeitgeber das Arbeitsverhältnis außerordentlich und fristlos. Dagegen wehrte sich der Arbeitnehmer mit dem Argument, das durch den heimlichen Einsatz der Keylogging-Technik gewonnene Datenmaterial sei rechtswidrig erworben worden und könne daher nicht als Grundlage für seine Kündigung dienen.

2. Hohe Anforderungen an heimliche Datenerhebung am Arbeitsplatz

Das Bundesarbeitsgericht entschied, dass eine derartige Ausspähung einen schweren Eingriff in das Grundrecht des Arbeitnehmers auf informationelle Selbstbestimmung darstelle. Dieses umfasse auch das Recht auf die eigene Bestimmung über Preisgabe und Verwendung seiner persönlichen Daten.[5] Das Bundesdatenschutzgesetz (BDSG) erlaubt in seinem § 32 Abs. 1 S. 2 eine Informationsgewinnung im Hinblick auf personenbezogene Daten ohne Einwilligung des Betroffenen nur unter strengen Voraussetzungen. Eine Datenerhebung und -nutzung darf danach einzig durchgeführt werden, wenn gegen den Arbeitnehmer ein konkreter Verdacht einer Straftat oder einer schweren Pflichtverletzung während der Arbeitszeit besteht und die Verarbeitung erforderlich ist. Dazu ist zu prü-

---

5 BAG, Pressemitteilung Nr. 31/17.

fen, ob das schutzwürdige Interesse des Beschäftigten an dem Ausschluss der Verarbeitung nicht die Informationsinteressen des Arbeitgebers überwiegen, insbesondere ob Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.

Die Richter waren der Auffassung, dass die Maßnahme des Arbeitgebers „ins Blaue hinein" durchgeführt wurde, ohne dass ein vorher objektiv begründeter Verdacht gegen den Arbeitnehmer bestand. Darüber hinaus ist die Verhältnismäßigkeit der Maßnahme in Frage zu stellen.[6] Vor dem Hintergrund der hohen Intensität des Eingriffs durch die heimliche Aufzeichnung sämtlicher Tastenanschläge und besuchter Webseiten käme als milderes Mittel zunächst eine Kontrolle im Beisein des Arbeitnehmers in Betracht.[7] Da die Aufzeichnung aus den genannten Erwägungen rechtswidrig war, lehnten die Richter die aus dem Keylogging gewonnenen Log-Dateien und Screenshots als Beweismittel ab und ließen die daraus gewonnenen Erkenntnisse bei der Urteilsfindung außen vor. Die übrigen Vorwürfe des Arbeitgebers und die in der Stellungnahme des Arbeitnehmers eingeräumten Hinweise rechtfertigten für sich keine Kündigung ohne vorherige Abmahnung, sodass die Kündigung für unwirksam befunden wurde.

III. Parallelen zu bisheriger Rechtsprechung

Es ist alles andere als überraschend, dass die aus einer heimlichen Überwachung des Arbeitnehmers gewonnenen Daten nicht verwertbar sind. Denn wertungsmäßig steht die Keylogging-Überwachung der verdeckten Videoüberwachung gleich.[8] Auch in diesem Zusammenhang wurde die Verwertbarkeit der personenbezogenen Daten und Erkenntnisse bereits in einem Urteil aus 2013 abgelehnt.[9] Geklagt hatte damals eine Kassiererin, die im Verdacht stand, Geldbeträge aus dem Kassenbestand entnommen zu haben. Die Bestimmung des § 32 Abs. 1 S. 2 BDSG lässt

---

6 So bereits die Vorinstanz LAG Hamm, Urteil vom 17.06.2016 – 16 Sa 1711/15.

7 LAG Hamm, Urteil vom 17.06.2016 – 16 Sa 1711/15, Rn. 40.

8 Stoffels, BAG zur Überwachung mittels Keylogger (Kommentar).

9 BAG, Urteil vom 21.11.2013 – 2 AZR 797/11, Rn. 49 ff.

eine personenbezogene Datenerhebung nur zur Aufdeckung von Straftaten zu, soweit der Eingriff erforderlich ist und dem Arbeitnehmer kein überwiegendes, schützenswertes Interesse zukommt. Hier muss das Interesse an der Verwertung der Videoaufnahmen mit dem Interesse der überwachten Person an ihrer informationellen Selbstbestimmung abgewogen werden. Die verdeckte Videoüberwachung setzt insofern einen konkreten Verdacht einer Straftat oder einer schweren Pflichtverletzung des Arbeitnehmers voraus und ist nur zulässig, sofern andere Mittel bereits ergebnislos ausgeschöpft wurden.[10] Auch hier konnte der Arbeitgeber nicht nachweisen, dass falsche Abrechnungen zuvor konkret auf das Verhalten der gekündigten Kassiererin zurückzuführen waren. Die dargestellten Grundsätze für eine heimliche Aufzeichnung am Arbeitsplatz wurden auch für die heimliche Überwachung durch Keylogger angewandt und bestätigen, dass an die Zulässigkeit einer heimlichen Überwachung vor dem Hintergrund der Grundrechte des Arbeitnehmers hohe Anforderungen gestellt werden.

IV. Rückenwind aus Straßburg

Auch der Europäische Gerichtshof für Menschenrechte stärkte in seinem kürzlich ergangenen Urteil die Arbeitnehmerrechte.[11] Ein Unternehmen hatte den Chat-Verlauf eines rumänischen Arbeitnehmers, der auf seinem Dienst-PC einen Messengerdienst nutzte, umfangreich aufgezeichnet. Auch Privatgespräche mit seinem Bruder und seiner Verlobten befanden sich unter den Aufzeichnungen. Aufgrund übermäßig privater Nutzung wurde ihm gekündigt. Nachdem er vor rumänischen Gerichten mit seiner Klage auf Weiterbeschäftigung scheiterte, entschied der Europäische Gerichtshof für Menschenrechte, dass diese Überwachung eines Dienst-Computers gegen das Recht auf Privatleben aus Art. 8 der Europäischen Menschenrechtskonvention verstößt und die Beweismittel aus diesem Grund nicht für die Begründung einer Kündigung genutzt werden dürfen.

---

10 BAG, Urteil vom 21.11.2013 – 2 AZR 797/11, Rn. 50.

11 EGMR, Case of Bărbulescu v. Romania. Application No. 61496/08.

V. Einordnung nach neuem Datenschutzrecht

Fraglich ist, ob das Urteil des Bundesarbeitsgerichts Bestand haben wird. Denn ab dem 25.05.2018 gilt in allen Mitgliedstaaten der EU die neue EU-Datenschutz-Grundverordnung (DS-GVO). Diese enthält selbst zwar keine spezifischen Regeln zum Arbeitnehmerdatenschutz. Durch eine Öffnungsklausel in Art. 88 DS-GVO wird den Mitgliedstaaten aber ermöglicht, eine detaillierte Ausgestaltung für die Verarbeitung personenbezogener Beschäftigtendaten vorzunehmen. Dabei kann dieser Themenkomplex sowohl gesetzlich als auch durch Tarifverträge oder Betriebsvereinbarungen geregelt werden.

Mit der Neuregelung des Arbeitnehmerdatenschutzes in § 26 BDSG-neu ist der deutsche Gesetzgeber diesem Auftrag nachgekommen. Personenbezogene Daten von Beschäftigten dürfen demnach nur verarbeitet werden, sofern dies für die Begründung, Durchführung oder Beendigung des Arbeitsverhältnisses erforderlich ist. Dies ist durch eine Verhältnismäßigkeitsabwägung zwischen den widerstreitenden Interessen von Arbeitgeber und Arbeitnehmer zu ermitteln. Zur Aufdeckung von Straftaten müssen darüber hinaus dokumentierte, tatsächliche Anhaltspunkte einen Verdacht begründen. Dies entspricht im Wesentlichen der bereits bestehenden Regelung des § 32 BDSG, sodass die Rechtsprechung Bestand haben wird.

Der heimliche Einsatz von Keyloggern oder anderen Überwachungs-Tools kann demnach auch zukünftig nicht auf diesen gesetzlichen Erlaubnistatbestand gestützt werden. Möglich ist es aber, die Überwachung offenzulegen und dahingehend eine Betriebsvereinbarung mit dem Betriebsrat abzuschließen oder eine Einwilligung einzuholen. Insbesondere für die Einwilligung ergeben sich jedoch hohe Anforderungen: Eine solche ist nur wirksam, wenn der Arbeitnehmer freiwillig entscheiden durfte, § 26 Abs. 2 BDSG-neu. Wegen des Abhängigkeitsverhältnisses zwischen Arbeitgeber und Arbeitnehmer ist dies im Einzelfall genau zu prüfen. Angenommen wird die Freiwilligkeit z. B. wenn die Einwilligung zu einem wirtschaftlichen oder rechtlichen Vorteil für den Arbeitnehmer führt, Erwägungsgrund 155. Dies wird jedoch oft nicht der Fall sein, sodass auch

die Möglichkeit, eine Einwilligung einzuholen, keine Rechtssicherheit für den Arbeitgeber verspricht.

VI. Keylogger auch Thema im US-amerikanischen Recht

Auch in den USA ist Keylogging am Arbeitsplatz bereits Gegenstand von Gesetzgebung und Rechtsprechung gewesen. Der US-amerikanische „Federal Wiretap Act" verbietet jedes absichtliche Abfangen von mündlichen, kabelgebundenen und elektronischen Kommunikationsdaten.[12] Abfangen meint dabei die akustische oder in sonstiger Weise durchgeführte Beschaffung elektronischer, kabelgebundener oder mündlicher Kommunikationsinhalte unter Einsatz elektronischer, mechanischer oder anderer Geräte. In einem ähnlichen Fall hat der Beklagte ebenfalls einen Keylogger auf dem Computer seines Mitarbeiters installiert und sich die Daten übermitteln lassen.[13] Ein kalifornisches Gericht entschied, dass ein Gerät oder Programm, das Kommunikationsdaten innerhalb eines Nutzersystems aufzeichnet, kein „Abfangen" im Sinne des Gesetzes darstelle.[14] Das US-amerikanische Gesetz reguliert danach gerade einige besonders gefährliche Spyware-Softwares – insbesondere die Keylogger-Software – nicht.[15] Eine höchstrichterliche Rechtsprechung dazu ist bislang nicht ergangen. Dennoch lässt sich auch hier erkennen, dass der Datenschutz auf nationaler und europäischer Ebene deutlich weitgehender ausgestaltet ist und umfassender schützt als in den Vereinigten Staaten.

VII. Fazit

Vermehrt ergeben sich Anwendungsszenarien für Big Data in den Personalabteilungen der Unternehmen. Die datenschutzrechtlichen Grenzen, die dabei zu beachten sind, wurden allerdings kürzlich vom Bundesarbeitsgericht betont. So ist der heimliche Einsatz von Keyloggern zur Datengewinnung unzulässig. Dadurch wurden die Persönlichkeitsrechte von

---

12 § 2511(1)(a) Federal Wiretap Act.

13 US v. Ropp 347 F. Supp. 2d 831 (C.D. Cal. 2004).

14 Bellia, Berkeley Technology Law Journal 2005, S. 1283, 1304.

15 Bellia, Berkeley Technology Law Journal 2005, S. 1283, 1304.

Arbeitnehmern gestärkt. Dies findet auch auf europäischer Ebene Resonanz – sowohl, wie ebenfalls kürzlich entschieden, nach der europäischen Menschenrechtskonvention, als auch nach dem zukünftig anwendbaren Regime der europäischen DS-GVO. So ist davon auszugehen, dass europäische datenverarbeitende Unternehmern – im Gegensatz zu ihren amerikanischen Kollegen – auch künftig Einwilligungen der Arbeitnehmer einholen müssen oder Betriebsvereinbarungen mit den Arbeitnehmervertretungen abschließen müssen, wenn sie Daten von Arbeitnehmern oder Bewerbern zu HR-Zwecken umfangreich auswerten wollen.

Literaturnachweise

Bellia, Sypware and the Limits of Surveillance Law, Berkeley Technology Law Journal 2005, Vol. 20, S. 1283-1343.

Ciampa, Security Awareness – Applying Practical Security in your World, 5. Auflage Boston 2017.

Gabler Wirtschaftslexikon, Stichwort: Keylogger, http://wirtschaftslexikon.gabler.de/Archiv/1408525/keylogger-v3.html.

Stoffels, BAG zur Überwachung mittels Keylogger (Kommentar), https://community.beck.de/2017/07/28/bag-zur-ueberwachung-mittels-keylogger.

Vogelsang/Hesser/Möllers, Hardware-Keylogger. Die Tastatur in der Hand des Feindes. DuD 2016, S. 729-734.

J. Ökonomische und juristische Aspekte des Mobile Payments (Christian Döpke und Philip Bitter)

Stand: Oktober 2018

Abstract: Mobile Payment

Von Bedeutung ist die Feststellung, dass Mobile Payment nicht mit Mobile Banking gleichzusetzen ist. Mobile-Payment-Anbieter nehmen zwar zu, jedoch bleiben die Nutzer auf dem deutschen Markt weitestgehend skeptisch – zumindest was die Einbindung von Smartphones angeht. Die Girocard der Deutschen Kreditwirtschaft ist bereits NFC-tauglich und funktioniert über das Bezahlverfahren „Girocard kontaktlos“ ohne vorherige Aufladung. Ein einheitlicher Standard hat sich bis dato zwar noch nicht durchgesetzt, die NFC-Technologie erscheint jedoch auch bei mobilen Endgeräten vielversprechend. Gerade für den stationären Handel verspricht Mobile Payment erhebliches Potential. Rechtlich gilt es vor allem bankaufsichtsrechtliche, vertragsrechtliche und datenschutzrechtliche Vorgaben zu beachten. Diese richten sich in erster Linie an die Zahlungsdienstleister.

I. Einleitung

Das weltweit erste kassenlose Lebensmittelgeschäft wurde von *Amazon* im Dezember 2016 in Seattle eröffnet. Darin erfassten Sensoren und Kameras die Einkäufe der Kunden, die später automatisch über das Smartphone abgerechnet wurden.[1] Ähnliche Beispiele finden sich in großer

[1] https://www.heise.de/newsticker/meldung/Amazon-Go-Amazon-eroeffnet-kassenloses-Lebensmittelgeschaeft-3559328.html (zuletzt abgerufen: 11/2018); allerdings zeigten sich hier noch erhebliche technische Probleme, sodass das Geschäft wieder geschlossen wurde und der breiten Öffentlichkeit auch zunächst verschlossen bleibt, siehe: https://www.heise.de/newsticker/meldung/Amazon-Go-mit-Schwierigkeiten-Kassenloses-Geschaeft-bleibt-geschlossen-3667380.html (zuletzt abgerufen: 11/2018).

Zahl: *Apple Pay* tritt in den deutschen Markt ein und *Google Pay* ist schon da.[2] Die *CINEPLEX-Gruppe* – immerhin in über 60 deutschen Städten mit Kinos vertreten – wird künftig bargeldlose Zahlungsprozesse vor Ort und online anbieten,[3] der schwedische Zahlungsdienstleister *Klarna* hat von der Finanzaufsicht eine Vollbanklizenz erhalten[4] und das irische FinTech-Unternehmen *Circle* bietet die Möglichkeit, kleine Geldbeträge ähnlich wie E-Mails, Fotos oder Textnachrichten via Smartphone zu verschicken.[5] Auch die großen deutschen Kreditinstitute bringen eigene Software-Lösungen zum mobilen Bezahlen auf den Markt, so etwa die Deutsche Bank oder die Postbank.[6]

Dieser Entwicklung zum Trotz hat sich, zumindest in Deutschland, Mobile Payment noch nicht etabliert. Nur etwa jeder vierte Kunde greift mindestens einmal im Monat auf entsprechende Apps zurück, 75 Prozent bevorzugen weiterhin die traditionellen Bezahlmethoden.[7] Gleichwohl lässt sich nicht bestreiten, dass dies nur eine Momentaufnahme ist und mobiles Bezahlen zukünftig an Bedeutung gewinnen wird. Immerhin können sich 46 Prozent aller Deutschen vorstellen, ihre Geldgeschäfte zukünftig fast ausschließlich bargeldlos abzuwickeln.[8] Die voranschreitende Durchdringung des Alltags mit Smartphones und dem Internet der Dinge beflügelt diese Entwicklung zusätzlich. Neuen Schwung dürfte vor allem die zunehmende Akzeptanz des Bezahlverfahrens „Girocard kontaktlos“

---

2 http://www.faz.net/aktuell/finanzen/digital-bezahlen/frueher-als-apple-google-pay-startet-in-deutschland-15659236.html (zuletzt abgerufen: 11/2018).

3 http://www.finanzen.net/nachricht/aktien/cineplex-gruppe-vertraut-zahlungsabwicklung-bs-payone-an-5741457 (zuletzt abgerufen: 11/2018).

4 https://www.springerprofessional.de/mobile-payment/bankenaufsicht/zahlungsdienstleister-klarna-startet-mit-banklizenz-durch/12458792 (zuletzt abgerufen: 11/2018).

5 http://www.live-pr.com/circle-macht-smartphone-zur-drehscheibe-f-r-r1050709674.htm (zuletzt abgerufen: 11/2018).

6 http://www.boerse-online.de/nachrichten/geld-und-vorsorge/Mobiles-Bezahlen-Mit-dem-Handy-gut-bei-Kasse-1005025805 (zuletzt abgerufen: 11/2018).

7 https://www.it-finanzmagazin.de/mobile-banking-und-mobile-wallets-in-deutschland-noch-nicht-angekommen-52524/ (zuletzt abgerufen: 11/2018).

8 https://www.bitkom.org/Presse/Presseinformation/Fast-jeder-Zweite-koennte-weitgehend-auf-Bargeld-verzichten.html (zuletzt abgerufen: 11/2018).

bringen, die eine kontaktlose Bezahlmöglichkeit an Point-of-Sale-Terminals (POS) mit der Girocard ermöglicht.[9]

Dies soll zum Anlass genommen werden, dem geneigten Leser im Folgenden zunächst einen Überblick über die technischen Hintergründe des Mobile Payment zu geben, um dann eine Analyse des ökonomischen Innovationspotentials vorzunehmen und ausgewählte juristische Fallstricke aufzuzeigen. Dabei sollen sich die Ausführungen auf die Besonderheiten bei Bezahlvorgängen mit mobilen Endgeräten wie Smartphones beschränken.

II. Begriffserklärung

Zunächst muss geklärt werden, was unter dem Begriff des Mobile Payments überhaupt zu verstehen ist.

Anders als bei der Barzahlung sind verschiedene Spielarten denkbar, die sowohl die verwendete Software als auch die verwendete Hardware betreffen. Das typische und verbindende Charakteristikum ist aber, dass ein mobiles Endgerät *direkt* zur bargeld- und kontaktlosen Abwicklung des Bezahlvorgangs eingesetzt wird.[10]

Das Mobile Payment im weiten Sinne erfasst dabei auch solche Zahlungen, die in räumlicher Distanz zum Zahlungsempfänger vorgenommen werden (sogenanntes Remote Payment) und vor allem im Onlinehandel Verwendung finden.[11]

Das Mobile Payment im engeren Sinne erfasst hingegen nur solche Zahlungen, die in räumlicher Nähe zum Zahlungsempfänger vorgenommen werden (sogenanntes Proximity Payment) und daher für den stationären Handel relevant sind.[12] Proximity-Payment-Lösungen sind nicht zwangsläufig auf das Smartphone beschränkt, denkbar sind beispielsweise auch mit Tankstellen-Zapfsäulen kommunizierende Smart Cars.[13]

---

9 https://www.girocard.eu/media/hintergrundinformationen_zu_girocard_kontaktlos.pdf (zuletzt abgerufen: 11/2018).

10 http://www.digitalwiki.de/mobile-payment/ (zuletzt abgerufen: 11/2018).

11 Baumann, GWR 2014, S. 493.

12 Brandenburg/Leuthner, ZD 2015, S. 111, 112.

13 http://www.car-it.com/rollende-kreditkarte/id-0051474 (zuletzt abgerufen: 11/2018).

Jedoch darf Mobile Payment nicht synonym mit dem Mobile Banking verstanden werden, da bei letzterem ein mobiles Endgerät lediglich als *Zugangsmedium* zum allgemeinen Internetportal einer Bank dient, aber ansonsten für den eigentlichen Bezahlvorgang keine Rolle spielt.[14]

III. Technische Funktionsweise

Im Proximity Payment verhält sich das mobile Endgerät des Kunden gegenüber dem Kassenterminal des Händlers, dem POS, wie eine Zahlungskarte.[15]

Zur beiderseitigen Kommunikation etabliert sich zunehmend die Near-Field-Communication-Technologie (NFC).[16] Dabei handelt es sich um einen Funkübertragungsstandard, über den – je nach Ausgestaltung[17] – eine kontaktlose Bezahlung vor Ort erfolgen kann.[18] Technische Voraussetzung ist, dass das verwendete mobile Endgerät einen sogenannten NFC-Controller besitzt, der die Modellierung der NFC-Signale ausführt.[19] Weiterhin wird ein sogenanntes Secure Element benötigt, das – anders als der Name vermuten lässt – nicht das Endgerät vor Angriffen schützen soll, sondern dem Speichern von Applikations- und Nutzungsdaten dient, ähnlich wie ein virtueller Tresor.[20] Eine ungeklärte Frage ist jedoch, wie das Secure Element flächendeckend integriert werden soll. Hierfür kommen grundsätzlich die SIM-Karte, eine externe Karte oder das mobile Endgerät selbst in Betracht.[21] Je nach Lösung haben unterschiedliche Parteien Zugriff und Verfügungsgewalt auf das Secure Element, bei SIM-

---

14 Schimansky/Bunte/Lwowski/Maihold, § 55, Rn. 4.

15 Rammos, CR 2014, S. 67, 68.

16 https://www.mobilepaymentstoday.com/articles/cashless-and-confident-growing-the-proximity-payment-market/ (zuletzt abgerufen: 11/2018).

17 Einen Überblick liefert der Leitfaden der BITKOM zur Mobile Wallet, https://www.bitkom.org/noindex/Publikationen/2014/Leitfaden/Mobile-Wallet/141105-Mobile-Wallet.pdf, S. 24 f. (zuletzt abgerufen: 11/2018).

18 Brandenburg/Leuthner, ZD 2015, S. 111, 112.

19 Kossel/Sokolov, c´t 3/2013, S. 74.

20 Rammos, ZD 2013, S. 599, 600.

21 Brandenburg/Leuthner, ZD 2015, S. 111, 112.

Karten-gebundenen Lösungen etwa die Mobilfunkanbieter[22], die hierfür jeweils eigene Interessen verfolgen.

Für die eigentliche Abrechnung schafft Mobile Payment kein neues Bezahlsystem, sondern nur ein neues Front End.[23] Der im Hintergrund ausgelöste Bezahlvorgang findet weiterhin über Lastschrift, Überweisung oder ähnliche Verfahren statt[24], wobei eine Abrechnung etwa über das Bank- bzw. Kreditkartenkonto oder auch die Rechnung des Telekommunikationsanbieters erfolgen kann.[25] Denkbar sind auch spezielle Smartphone-Only-Konten.

IV. Ökonomische Interessenabwägung

Vereinzelt wird angenommen, dass Mobile-Payment-Transaktionen bis zum Jahr 2020 Erlöse in Höhe von mehr als 1 Mrd. Euro erzielen sollen.[26] Inwiefern diese Größenordnung realistisch ist, kann aber kaum abgeschätzt werden. Dass der stationäre Handel mit innovativen Konzepten aufwarten muss, um sich gegen den Onlinehandel zu behaupten, zeigt aber nicht zuletzt eine Umfrage, wonach 23 Prozent der Deutschen den stationären Handel für entbehrlich halten.[27]

Als Argument für den Einsatz von Mobile Payment wird vorgebracht, dass dadurch eine schnellere Abwicklung des Bezahlvorgangs ermöglicht werde und sich gleichzeitig der administrative Aufwand, Bargeld zu zählen und vorrätig zu halten, verringere.[28] Dies als zutreffend unterstellt, kann Mobile Payment tatsächlich ein innovativer Wirtschaftsmotor sein, insbesondere, wenn sich weitere positive ökonomische Effekte auftun.

Diese können bspw. darin zu sehen sein, dass Mobile Payment den Händlern die Möglichkeit eröffnet, neue Kundenkreise zu erschließen,

---

22 Brandenburg/Leuthner, ZD 2015, S. 111, 113.

23 Busch, GewArch Beilage WiVerw, S. 148, 149.

24 Baumann, GWR 2014, S. 493, 494.

25 Rammos, CR 2014, S. 67, 68.

26 Baumann, GWR 2014, S. 493.

27 http://www.gfm-nachrichten.de/news/single-loca/article/jeder-vierte-deutschen-koennte-auf-stationaeren-handel-verzichten.html (zuletzt abgerufen: 11/2018).

28 Brandenburg/Leuthner, ZD 2015, S. 111, 112.

etwa aus dem Milieu der Digital Natives oder bei Touristengruppen, vor allem aus dem asiatischen Raum.[29] Für Reisende und insbesondere für Vielreisende bietet sich der Vorteil, vor Reiseantritt kein Bargeld mehr umtauschen zu müssen, da selbst Kleinstbeträge, wie etwa im Taxi oder beim Bäcker, mobil und in Sekundenschnelle[30] beglichen werden können.[31]

Positiv wird auch hervorgehoben, dass Mobile Payment mehr Privatsphäre gewähre als beispielsweise das Bezahlen mittels EC- oder Kreditkarte, da es nicht die Preisgabe personenbezogener Daten erfordere.[32] Dabei darf aber nicht übersehen werden, dass durch den Einsatz entsprechender Zusatzangebote eine noch bessere Analyse des Einkaufsverhaltens ermöglicht wird.[33] Auf diese Weise können nicht nur tagesaktuelle und passgenaue Angebote unterbreitet, sondern auch abwanderungswillige Kunden identifiziert werden. Der Händler kann also sein Kundenbeziehungsmanagement noch individueller gestalten und so eine neue Form der Kundenbindung erzeugen.

Bedenkenswert ist, dass die Anschaffung einer POS-Software für den Händler eine erhebliche Investition darstellt, die sich langfristig aber auch durch das Entfallen der Vorhaltekosten für Bargeld rentieren kann.

Letztlich entscheidet über die ökonomischen Vor- und Nachteile vor allem die Akzeptanz des Verbrauchers. Diese wird wesentlich durch sein Vertrauen in die Technologie gebildet.[34]

---

29 2016 wurden 2,58 Millionen Übernachtungen chinesischer Touristen in Deutschland gezählt. Gerade in China sind Mobile Payment Lösungen weit verbreitet, siehe https://www.it-finanzmagazin.de/jetzt-auch-noch-wechat-pay-wirecard-bringt-alipay-konkurrenten-nach-europa-53080/ (zuletzt abgerufen: 11/2018), sodass entsprechende Angebote die Konsumfreudigkeit auch in Deutschland begünstigen können.

30 Knops/Wahlers, BKR 2013, S. 240, 241.

31 Unerlässlich ist dazu freilich, dass sich ein weltweiter technischer Standard durchsetzt.

32 http://www.techgyd.com/7-pros-cons-mobile-payments-must-know/17057/ (zuletzt abgerufen: 11/2018).

33 Baumann, GWR 2014, S. 493.

34 Busch, GewArch Beilage WiVerw, S. 148, 149.

V. Juristische Hürden

Zur Wahrung der Rechtssicherheit und Chancengleichheit müssen einige juristische Vorgaben beachtet werden – vor allem solche bankaufsichtsrechtlicher, vertragsrechtlicher und datenschutzrechtlicher Art.

Da das mobile Bezahlen ein relativ neues Phänomen ist, fehlte es zunächst an klaren Regelungen. Erkannt wurde der erhebliche Regulierungsbedarf inzwischen auf europäischer Ebene, was zur Verabschiedung der zweiten (und vollharmonisierenden) Zahlungsdiensterichtlinie (PSD2)[35] geführt hat, die durch das Zahlungsdiensteumsetzungsgesetz (ZDUG)[36] Einzug vor allem in das Bürgerliche Gesetzbuch (BGB) und das neu geordnete Zahlungsdiensteaufsichtsgesetz (ZAG) gehalten hat.

1. Bankaufsichtsrechtliche Erwägungen

Seit der Richtlinie über Zahlungsdienste im Binnenmarkt[37] ist der Zahlungsverkehrsmarkt nicht mehr nur Kredit- und Finanzdienstleistungsinstituten vorbehalten, sondern auch für Nichtbanken geöffnet.

Die Umsetzung des aufsichtsrechtlichen Teils der Richtlinie erfolgte in Deutschland mit dem ZAG.[38] Dieses stellt die Anbieter von Zahlungsdiensten zwar unter die Aufsicht der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin), unterwirft sie aber weniger strengen Regelungen als dies bei Kredit- und Finanzdienstleistungsinstituten im Sinne des Kreditwesengesetzes (KWG) der Fall ist.[39]

---

35 Richtlinie (EU) 2015/2366, worauf in Deutschland das Gesetz zur Umsetzung der Zweiten Zahlungsdiensterichtlinie folgt.

36 Gesetz zur Umsetzung der Zweiten Zahlungsdiensterichtlinie v. 17. Juli 2017, BGBl. I 48, 2446.

37 RL 2007/64/EG vom 13.11.2007; inzwischen aufgehoben durch RL (EU) 2015/2366.

38 Die Richtlinie enthielt auch vertragsrechtliche Bestimmungen, die in den §§ 675c ff. BGB Niederschlag gefunden haben. Mit der Umsetzung der RL (EU) 2015/2366 wurde das ZAG entsprechend geändert.

39 Baumann, GWR 2014, S. 493, 494.

Zur Anwendbarkeit des ZAG ist zunächst erforderlich, dass ein sogenannter Zahlungsdienstleister handelt.[40] Darunter ist gem. § 1 Abs. 1 S. 1 Nr. 1 ZAG auch ein Zahlungsinstitut zu fassen, das als Unternehmen legaldefiniert wird, „das gewerbsmäßig oder in einem Umfang, der einen in kaufmännischer Weise eingerichteten Geschäftsbetrieb erfordert, Zahlungsdienste erbringt". Zahlungsdienste sind in § 1 Abs. 1 S. 2 ZAG legaldefiniert. Für Mobile-Payment-Lösungen griff vor der Umsetzung der PSD2 die frühere Nr. 5[41], wonach ein sogenanntes digitalisiertes Zahlungsgeschäft vorlag, wenn „die Ausführung von Zahlungsvorgängen, bei denen die Zustimmung des Zahlers zur Ausführung eines Zahlungsvorgangs über ein Telekommunikations-, Digital- oder IT-Gerät übermittelt wird und die Zahlung an den Betreiber des Telekommunikations- oder IT-Systems oder IT-Netzes erfolgt, sofern der Betreiber ausschließlich als zwischengeschaltete Stelle zwischen dem Zahlungsdienstnutzer und dem Lieferanten der Waren oder Dienstleistungen tätig ist".[42] Mit Umsetzung der PSD2 gehen das sog. Zahlungsauthentifizierungsgeschäft und digitalisierte Zahlungsgeschäft in § 1 Abs. 1 S. 2 Nr. 5 ZAG, dem Akquisitionsgeschäft, auf vgl. § 1 Abs. 35 ZAG.

Anbieter von Mobile-Payment-Lösungen werden auf ebendiese Weise tätig, etwa wenn sie die NFC-Technologie einsetzen.[43] Als Zahlungsinstitut müssen sie vor Aufnahme der Geschäftstätigkeit grundsätzlich eine schriftliche Tätigkeitserlaubnis der BaFin erhalten, § 10 Abs. 1 ZAG. Damit diese erteilt werden kann, muss ein formaler Voraussetzungskatalog erfüllt sein, § 10 Abs. 2 Nr. 1-17 ZAG. § 63 Abs. 1 Nr. 4 bzw. 5 ZAG statuieren für diesen Fall Freiheits- und Geldstrafen.

Gem. § 55 Abs. 1 S. 1 Nr. 2 ZAG[44] ist der Zahlungsdienstleister nunmehr verpflichtet, „eine starke Kundenauthentifizierung zu verlangen, wenn der

---

40 Für Mobile Payment-Lösungen können auch die Regelungen für das E-Geld-Geschäft relevant sein.

41 Beziehungsweise je nach Ausgestaltung die Nr. 6 (Finanztransfergeschäft), auf deren Darstellung aus Gründen der Lesbarkeit und des Umfangs dieses Beitrags verzichtet wird.

42 Vertiefend Casper/Terlau, § 1, Rn. 63 ff.

43 Vgl. Diekmann/Wieland, ZBB 2011, S. 297.

44 In Umsetzung von Art. 97 Abs. 1 PSD2.

Zahler einen elektronischen Zahlungsvorgang auslöst.“ Die Autorisierung muss dabei grundsätzlich auf zwei von drei Elementen der Kategorie Wissen, Besitz und Inhärenz beruhen, vgl. Art. 4 Abs. 1 VO (EU) 2018/389. Ausnahmen i.S.v. § 55 Abs. V ZAG regelt jedoch Art. 11 VO (EU) 2018/389 gerade für das Auslösen eines kontaktlosen elektronischen Zahlungsvorgangs, wenn der Einzelbetrag nicht über 50 Euro hinausgeht (a), und die früheren kontaktlosen Zahlungsvorgänge seit der letzten starken Authentifizierung nicht über 150 Euro hinausgehen (b).

Neben dem ZAG sind auch Regelungen des Geldwäschegesetzes (GwG) zu beachten. Nach dem dort normierten § 2 Abs. 1 Nr. 3 gelten Zahlungs- und E-Geld-Institute im Sinne des ZAG als Verpflichtete, weshalb sie u.a. zur Verhinderung von Geldwäsche über ein wirksames Risikomanagement verfügen müssen, § 4 Abs. 1 GwG und bestimmte Sorgfaltspflichten zu beachten haben, §§ 10 ff. GwG.

2. Vertragsrechtliche Aspekte

Das Verhältnis zwischen einem Verbraucher und den Anbietern von Mobile-Payment-Lösungen ist als Zahlungsdienstevertrag im Sinne von § 675f BGB zu qualifizieren.

Von zentralem Interesse sind vertragsrechtlich die Haftungsvorschriften im Fall von nicht autorisierten Zahlungsvorgängen (vgl. § 675j BGB). Einschlägig ist dafür § 675u BGB, wonach grundsätzlich der Zahlungsdienstleister haftet; er hat gegen den Zahler keinen Anspruch auf Erstattung seiner Aufwendungen (Abs. 1 S. 1) und ist verpflichtet, diesem den Zahlungsbetrag unverzüglich zu erstatten (Abs. 1 S. 2).

Anders ist die Lage zu beurteilen, wenn die nicht autorisierte Zahlung auf der Nutzung eines verlorengegangenen, gestohlenen oder sonst abhandengekommenen Zahlungsauthentifizierungsinstruments – etwa einem Smartphone mit NFC-Technologie[45] – beruhen. Dann greift nämlich § 675v BGB, der dem Zahlungsdienstleister einen Schadensersatzanspruch gegen den Zahler gewährt. Trifft Letzterer grob fahrlässig nicht

[45] Auch der Diebstahl eines Smart Cars kann damit ganz neue Dimensionen annehmen.

alle zumutbaren Vorkehrungen, um die personalisierten Sicherheitsmerkmale, beispielsweise Sicherheitscodes, vor unbefugtem Zugriff zu schützen, ist der Anspruch der Höhe nach nicht begrenzt. Ein solcher Fall läge etwa vor, wenn bei einem Mobiltelefon mit NFC-Technik die Zugangscodes direkt im Gerät gespeichert würden.[46]

Gleichzeitig obliegt es dem Zahlungsdienstleister, für eine dem Stand der Technik entsprechende hinreichende Verschlüsselung des Datenverkehrs zu sorgen[47], um Schadsoftware und Phishing-Attacken vorzubeugen.[48]

3. Datenschutzrechtliche Erwägungen

Da der Eintritt von Unternehmen wie *Amazon*, *Apple* oder auch *Google* auf den Zahlungsdienstemarkt vor allem aus Interesse an den Transaktionsdaten erfolgt, muss ein zukunftsorientiertes Zahlungsdiensterecht in besonderem Maße Datenschutzrecht sein.[49]

Sofern personenbezogene Daten erhoben, verarbeitet oder genutzt werden, sind die datenschutzrechtlichen Bestimmungen zu beachten. Für die Zahlungsabwicklung mit NFC-Technologie ist das besonders deshalb relevant, weil die notwendigerweise gespeicherten Log-Dateien u.a. Informationen über die letzten Abbuchungs- und Rückbuchungstransaktionen sowie Karten- und Kundennummer enthalten.[50] Dies hat der Düsseldorfer Kreis zum Anlass genommen, darauf hinzuweisen, dass durch technisch-organisatorische Maßnahmen ein unberechtigtes Auslesen der Daten durch Dritte zu verhindert werden muss.[51] Da durch den Einsatz von NFC-Technologie verschiedene Parteien an einem Bezahlvorgang betei-

---

46 Säcker et al./Jungmann, § 675l, Rn. 43.

47 Busch, GewArch Beilage WiVerw, S. 148, 152.

48 Schütte, DuD 2014, S. 20, 23.

49 Busch, GewArch Beilage WiVerw, S. 148, 153 f.

50 m.w.N. Rammos, CR 2014, S. 67, 71.

51 Beschluss vom 18./19.09.2012, https://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/19092012NFCBeiGeldkarten.html?cms_templateQueryString=nfc&cms_sortOrder=score+desc (zuletzt abgerufen: 11/2018).

ligt sind, stellt sich zudem die Frage, wer als Verantwortlicher zu qualifizieren ist.[52] Nach Art. 4 Nr. 7 DS-GVO[53] ist darunter die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle zu verstehen, „die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet." In aller Regel wird dies der Zahlungsdienstleister sein.

VI. Fazit

Für ein funktionierendes Wirtschaftssystem sind vor allem effiziente und sichere Zahlungssysteme essentiell.[54] Als ein solches sich neu am Markt etablierendes kann das Mobile Payment gesehen werden, das vor allem für den stationären Handel großes Potential bietet. Die rechtlichen Hürden treffen dabei in erster Linie den Zahlungsdienstleister und weniger den Händler vor Ort.[55]

Gerade vor dem Hintergrund, dass durch das Internet der Dinge die potentielle Zahl der Zahlungsgeräte unbegrenzt erscheint, muss sich aber ein technischer Standard etablieren, der das Vertrauen der Nutzer sichert.

Literaturnachweise

Baumann, Mobile Payment – neuer Wein in alten Schläuchen? GWR 2014, S. 493-496.

Brandenburg/Leuthner, Local Commerce – Einsatz von Mobile Payment-Lösungen – Neue Zahlungsmethoden für den stationären Handel, ZD 2015, S. 111-115.

Busch, Mobile Payment – Rechtliche und technische Rahmenbedingungen für Innovationen im Zahlungsverkehr, GewArch Beilage WiVerw 2014, S. 148-154.

Casper/Terlau, Kommentar zum ZAG, München 2014.

---

52 Rammos, ZD 2013, S. 599, 600.

53 Der Begriff des Verantwortlichen unterscheidet sich damit vom bisherigen Begriff der „verantwortlichen Stelle" in § 3 Abs. 7 BDSG a.F.

54 Knops/Wahlers, BKR 2013, S. 240.

55 Brandenburg/Leuthner, ZD 2015, S. 111, 115.

Diekmann/Wieland, Der neue aufsichtsrechtliche Rahmen für das E-Geld-Geschäft, ZBB 2011, 297-304.

Knops/Wahlers, Evolution des Zahlungsverkehrs durch Mobilepayment – am Beispiel von M-Pesa, BKR 2013, S. 240-243.

Kossel/Sokolov, Das Handy als Brieftasche, c't 3/2013, S. 74-77.

Rammos, Kontaktlose Zahlungen mittels mobiler Endgeräte, ZD 2013, S. 599-603.

Rammos, The future is near ... field communication?, CR 2014, S. 67-72.

Säcker/Rixecker/Oetker/Limperg, Münchener Kommentar zum BGB, Band 6, 7. Auflage München 2018.

Schimansky/Bunte/Lwowski, Bankrechts-Handbuch, 5. Auflage München 2017.

Schütte, NFC? Aber sicher, DuD 2014, S. 20-24.

K. Alexa, Siri & Google Assistant – was ist erlaubt? Sprachassistenten und das Recht (Henning Brockmeyer & Verena Vogt)

Stand: März 2018

Abstract: Alexa & Co.

Sprachassistenten halten Einzug in unser Zuhause und mit ihnen die Tech-Giganten. Unsere Welt wird smarter. Doch was ist der Preis? Gefühlt ist der Gewinn an Komfort durch Licht und Musik auf Zuruf teuer erkauft. Privatsphäre erscheint als Relikt vergangener Zeit. Ersthilfe könnte die seit 25.05.2018 geltende Datenschutz-Grundverordnung bieten. Doch damit nicht genug. Der fortschreitende Wandel fordert das Recht. Haftung für Schäden durch autonom agierende Assistenten und der Vertragsschluss mit ihnen sind die derzeit wohl wichtigsten zu klärenden Vorboten zukünftiger Entwicklungen im Bereich der intelligenten Assistenz.

I. Alles easy?

Spätestens seit dem Weihnachtsfest 2017 dürfte es auch in vielen deutschen Haushalten vielfach zu hören sein: „Alexa, … !?“[1] Sprachassistenten wie beispielsweise Amazons Alexa, Apples Siri oder Googles Assistant ziehen mehr und mehr in unseren Alltag ein und mit ihnen die datengetriebenen Tech-Giganten. Die Entwickler der Sprachassistenten versprechen eine smarte Welt. Eine einfache Frage oder ein kurzer Befehl an den Assistenten und das Licht geht an, die gewünschte Musik wird abgespielt oder die Wetterprognose berichtet. Sprachassistenten

[1] Amazons Echo Dot und Fire TV-Stick mit Alexa-Sprachfernbedienung waren im Weihnachtsgeschäft 2017 über alle Kategorien hinweg die meistverkauften Produkte auf amazon.com, vgl: https://amazon-presse.de/Top-Navi/Pressetexte/Pressedetail/amazon/de/Produkte/171227_WrapUp/ (zuletzt abgerufen: 11/2018); genaue Verkaufszahlen veröffentlicht Amazon aber nicht.

finden sich heute bereits in Smartphones, Lautsprechern, Autos und Kinderspielzeug und in Zukunft sehr wahrscheinlich auch noch in deutlich mehr Produkten. Unsere neuen smarten Helfer bieten ohne Tippen schnellen Zugriff auf Informationen aus dem Netz, vereinfachen die Bedienung vieler technischer Geräte und ermöglichen mitunter schon heute den Kauf von Produkten oder in den USA sogar das Online-Banking.[2] Doch welchen Preis hat dieser Komfortgewinn und welche neuen rechtlichen Fragen stellen sich im Zusammenhang mit Alexa und Co.? Dieser Beitrag soll im Überblick kurze Antworten auf die derzeit drängendsten Fragen in diesem Kontext geben.

II. Alexa, wie funktionierst du?

Sprachassistenten nehmen mittels eingebauter Mikrofone dauerhaft oder nach Aktivierung ihre Umgebung auf. Im Falle von Amazons intelligenter Lautsprecherfamilie Echo, die hier aus Gründen der Bekanntheit exemplarisch zugrunde gelegt sei, erfolgt während der Daueraufnahme eine geräteinterne Stichworterkennung. Wird ein hinterlegtes Aktivierungswort wie zumeist „Alexa“ erkannt, beginnt der eigentliche Verarbeitungsprozess. Der Sprachassistent sendet nun die nach dem Aktivierungswort aufgenommenen Sprachdaten an die Server von Amazon (sog. Cloud). Dort wertet eine komplexe Software die erlangten Audiodaten in Echtzeit aus und übermittelt eine Antwort, die als Sprachausgabe erfolgt.[3]

III. Meine Daten!

Dieses Vorgehen produziert viele Informationen über den Nutzer. Neben der Sprachaufzeichnung als solcher werden auch die IP-Adresse des Nutzers, Daten über das verwendete Endgerät sowie Such- und Shopping-Informationen an die Cloud geschickt.[4] Aussagekräftig in Bezug auf den Nutzer und seine Interessen ist weiterhin insbesondere auch der

---

2 https://www.usbank.com/newsroom/news/customers-can-now-complete-banking-tasks-with-us-bank-skill-for-amazon-alexa.html (zuletzt abgerufen: 11/2018).

3 https://www.amazon.de/gp/help/customer/display.html?nodeId=201602230 (zuletzt abgerufen: 11/2018).

4 Heidrich/Maekler, c’t 22/2017, S. 86.

Inhalt der dem Sprachassistenten gestellten Frage sowie dessen Antwort. Zusammen mit Daten aus anderen Quellen könnten Nutzerprofile für Marketing und Marktforschungszwecke gemäß § 15 Abs. 3 Telemediengesetz (TMG) erstellt werden. Hierauf weist auch die Bundesbeauftragte für den Datenschutz, Andrea Voßhoff, hin.[5] Per se muss das nicht schlecht sein. Wissen ist aber bekanntlich Macht und wer kann schon sagen, ob beispielsweise Apple in Zukunft den kredit-finanzierten Kauf eines iCar nicht von der Interaktion des Nutzers mit Siri abhängig macht.[6]

1. Neue Transparenz

Die Dimension der Möglichkeiten Erkenntnisse aus Daten zu erlangen und der Ort der Verwendung ist in Zeiten der sprachassistierenden Cloud für den Nutzer kaum fassbar. Doch wie gelangt mehr Transparenz in das Dickicht der Datenflut? Nach Art. 8 Abs. 2 S. 1 der Charta der Grundrechte der Europäischen Union (Schutz der personenbezogenen Daten) dürfen personenbezogene Daten nur nach Treu und Glauben verarbeitet werden. Wesentliche Ausprägung dieses Grundsatzes ist mitunter, dass der Betroffene die maßgeblichen Faktoren der Verarbeitung seiner Daten nachvollziehen können muss.[7] Erst hierdurch wird es ihm möglich zu reagieren. Dies erfordert aber, dass der Nutzer weiß, dass seine Daten verarbeitet werden. Genau dies ist das besondere Anliegen der seit 25.05.2018 in allen EU-Mitgliedstaaten unmittelbar geltenden Datenschutz-Grundverordnung (DS-GVO). Diese fordert Transparenz bei der Datenverarbeitung, Art. 5 Abs. 1 lit. a DS-GVO. Damit diese Transparenz den Nutzer auch erreicht, verpflichtet Art. 13 DS-GVO denjenigen der personenbezogene Daten erhebt, den Betroffenen zum Zeitpunkt der Erhebung darüber zu informieren, dass es zu einer Datenverarbeitung kommt, zu welchem Zweck sie erfolgt, wer der Verantwortliche ist und wie der Betroffene diesen erreichen kann. Gerade gegenüber den auch

---

5 https://www.bfdi.bund.de/SharedDocs/Publikationen/DatenschutzKompaktBlaetter/Sprachassistenten.html?cms_templateQueryString=sprachassistenten&cms_sortOrder=score+desc (zuletzt abgerufen: 11/2018).

6 https://www.theatlantic.com/technology/archive/2015/06/listening-machines/396179/ (zuletzt abgerufen: 11/2018).

7 Schantz/Wolff, Rn. 1149.

in der Privat- und Intimsphäre datensammelnden Sprachassistenten ist der Nutzer darauf angewiesen, dass Informationspflichten die Informationsasymmetrie zwischen den Tech-Giganten und dem Nutzer verringern.[8] Doch damit nicht genug: Bereits im Entwicklungsstadium eines smarten Produkts muss nun immer gemäß Art. 25 Abs. 1 DS-GVO der Datenschutz berücksichtigt werden (sog. privacy by design). Im Übrigen dürfen intelligente Produkte nun auch nur noch mit einer datenschutzfreundlichen Voreinstellung ausgeliefert werden, Art. 25 Abs. 2 DS-GVO (sog. privacy by default).

2. Ja, ich will!

Der Datenschutz kennt aber auch in Zeiten der DS-GVO Grenzen. Zwar erfordert Art. 6 Abs. 1 lit. a DS-GVO die Einwilligung des Betroffenen in die Datenverarbeitung. Doch was ist mit Dritten, beispielsweise Besuchern? Insoweit gibt es eine datenschutzrechtliche Schwachstelle der digitalen Assistenten, die bislang nicht auf eine einzelne einwilligende Person trainiert werden können.[9] Problematisch ist in Hinblick auf die Einwilligung des Nutzers weiter auch, dass dieser nicht in die unbewusste Aktivierung eines Sprachassistenten beispielsweise durch einen Fernseher, das Radio oder andere Geräte einwilligt. Anfang 2017 machte sich Burger King in den USA genau diese Unzulänglichkeit der Sprachassistenten zu Nutzen und kreierte einen 15-sekündigen Spot, der damit endete über den Fernseher den Google Assistant aufzufordern die Vorzüge des Whopper-Burgers anzupreisen. Hierfür war zuvor der stets in diesem Fall via Google Home wiedergegebene Wikipedia-Artikel von Burger King entsprechend einer Werbebotschaft optimiert worden.[10] Auch weiterhin wird wohl alles was nach Ermittlung des Aktivierungswortes durch einen Sprachassistenten vernommen wird, aufgezeichnet, verarbeitet und gespeichert. In diesem Zusammenhang ist es im Übrigen kritisch zu sehen, dass Sprachassistenten auch durch ähnlich klingende Begriffe wie im Falle von Alexa beispielsweise durch den Namen „Alexander“ aktiviert

---

8 Schantz/Wolff, Rn. 1149.

9 Heidrich/Maekler, c’t 22/2017, S. 86.

10 http://www.spiegel.de/netzwelt/gadgets/burger-king-werbung-fuer-google-home-ok-burger-king-ihr-habt-versagt-a-1143193.html (zuletzt abgerufen: 11/2018).

werden können.[11] Diese Erfahrung mussten zum Beispiel auch zwei Amerikaner machen. Alexa hatte eine Unterhaltung des Ehepaars aus Oregon aufgezeichnet und an einen Mitarbeiter der Firma des Ehemanns geschickt. Laut Amazon soll dieses „unwahrscheinliche" Ereignis dadurch entstanden sein, dass Alexa aus der Unterhaltung Wörter verstanden haben soll, die den entsprechenden Aktivierungs- und Schlüsselwörtern ähnlich gewesen sein sollen.[12]

Sichere Abhilfe vor ungewolltem „Belauscht-werden" schafft daher nur ein Bewusstsein, sich insbesondere in fremder Umgebung zu vergewissern, ob Sprachassistenten aktiv sind und diese gegebenenfalls zu deaktivieren.

3. Cayla ging zu weit

Dass Sprachassistenten immer tiefer in die Privatsphäre der Nutzer eindringen und es bereits bis in die Kinderzimmer geschafft haben, wurde deutschlandweit bekannt, als die Bundesnetzagentur zu Beginn des letzten Jahres die Spielzeugpuppe My Friend Cayla als nach § 90 Telekommunikationsgesetz (TKG) verbotene Sendeanlage einstufte.[13] Cayla verfügte über ein Mikrofon und einen Lautsprecher. Mittels Bluetooth kommunizierte sie mit einer Smartphone-App. Leuchtete ihre Halskette, war sie online und Kinder konnten mit ihr in Dialog treten.[14] Im Rechtssinne galt sie als Sendeanlage, da die Übertragung der Audiodaten per Funk erfolgte. Weil zudem für Kinder, Eltern und Dritte nicht ohne Weiteres ersichtlich war, dass in Caylas Innerem ein Mikrofon lauscht, lag auch die für § 90 Abs. 1 TKG erforderliche Tarnung vor. Die Einführung, der Besitz

---

11 https://www.verbraucherzentrale.nrw/sites/default/files/2017-12/17-12-20_PM_Spracherkennung.pdf (zuletzt abgerufen: 11/2018).

12 http://www.sueddeutsche.de/digital/amazon-echo-alexa-verschickt-privatgespraech-an-mitarbeiter-des-ehemanns-1.3991757 (zuletzt abgerufen: 11/2018).

13 https://www.bundesnetzagentur.de/SharedDocs/Pressemitteilungen/DE/2017/14012017_cayla.html;jsessionid=6D0157245ABD2594236EC56A4780DF12?nn=690686 (zuletzt abgerufen: 11/2018).

14 http://www.zeit.de/digital/datenschutz/2017-02/my-friend-cayla-puppe-spion-bundesnetzagentur (zuletzt abgerufen: 11/2018).

und die Verbreitung einer solchen getarnten Sendeanlage ist in Deutschland gemäß § 90 Abs. 1 TKG verboten und nach § 148 Nr. 2 TKG auch strafbar, weshalb Cayla vom Markt genommen werden musste. Caylas Erscheinung war typisch für Sprachassistenten, die überwiegend in attraktiven Gadgets verpackt und mit angenehmer meist weiblicher Stimme um die Gunst des Nutzers werben.[15]

4. Hüte dich vor Manipulation!

Der Umstand, dass Sprachassistenten systembedingt dauerhaft mit dem Internet verbunden sein müssen, macht sie anfällig für Manipulation. Wie oben bereits ausgeführt, haben Sprachassistenten über Online-Banking oder Online-Shopping Zugriff auf Kontodaten der Nutzer, weshalb im Falle eines Hacker-Angriffs auch finanzielle Verluste entstehen können. Auf dieses Risiko weist die Bundesbeauftragte für den Datenschutz ausdrücklich hin.[16] Zudem liegt es nahe, dass sich auch die Sicherheit der in der Cloud gespeicherten „gesprochenen" Daten nicht umfassend gewährleisten lässt. Dies vor dem Hintergrund, dass beispielsweise Apple bereits in den AGB seiner normalen iCloud weder zusichert noch garantiert, dass der Dienst frei von Verlusten, Beschädigungen, Angriffen, Viren, Eingriffen, Angriffen durch Hacker oder anderen sicherheitsrelevanten Störungen sein wird und Apple in diesem Zusammenhang jegliche Haftung ausschließt.[17] Weniger bedrohlich, aber dennoch ein Risiko sind Angriffe, die eine räumliche Nähe zum smarten Lautsprecher voraussetzen. Sicherheitsforschern ist es gelungen Bluetooth-Schwachstellen bei Geräten von Amazon und Google zu finden, die eine komplette Übernahme des Geräts ermöglichen. Insoweit machten sie sich zu Nutze, dass die Geräte ständig über Bluetooth nach

---

15 https://www.theatlantic.com/technology/archive/2015/06/listening-machines/396179/ (zuletzt abgerufen: 11/2018).

16 https://www.bfdi.bund.de/SharedDocs/Publikationen/DatenschutzKompaktBlaetter/Sprachassistenten.html?cms_templateQueryString=sprachassistenten&cms_sortOrder=score+desc (zuletzt abgerufen: 11/2018).

17 https://www.apple.com/legal/internet-services/icloud/de/terms.html (zuletzt abgerufen: 11/2018).

Kommunikationspartnern suchen. Beide Hersteller haben aber zwischenzeitlich Updates veröffentlicht, die diese Sicherheitslücke schließen.[18]

IV. Alexa, kaufst du oder ich?

Neben der Frage des Datenschutzes digitaler Sprachassistenten stellt sich im Weiteren die Frage, wann im Falle des sprachassistierten Shoppings der Nutzer eigentlich kauft. Grundsätzlich erfordert ein Vertragsschluss ein Angebot und eine Annahme. Fragt der Sprachassistent, ob man die Ware kaufen möchte, kann darin ein Angebot zum Vertragsschluss liegen. Die Antwort „Ja“ stellt dann die Annahme dar.[19] Alternativ könnte in der Frage des Assistenten auch bloß eine Aufforderung an den Nutzer liegen, seinerseits ein Angebot abzugeben (sog. invitatio ad offerendum). Gibt der Nutzer wie soeben vorgezeichnet eine Bestellung auf, würde der Kaufvertrag dann beispielsweise durch die Versandbestätigung per Mail oder spätestens mit dem Versenden der Ware abgeschlossen. Ob der eine oder andere Weg zum Vertragsschluss beschritten wird, richtet sich in der Regel nach den Nutzungsbedingungen (AGB) der Versandunternehmen.[20] Im Falle von Alexa gibt der Nutzer ausweislich der AGB von Amazon, die auch auf den Spracheinkauf über Alexa Anwendung finden[21] mit seiner gesprochenen Bestellung ein Angebot ab, dessen Eingang Amazon zunächst mit einer unverbindlichen Bestellbestätigung bestätigt. Grundsätzlich kann die Annahme konkludent durch das Versenden der bestellten Ware erfolgen.[22] Im Fall von Amazon bestimmen die AGB, dass der Kaufvertrag dann zustande kommt, wenn sowohl das bestellte Produkt an den Nutzer versendet als auch der Versand mit einer zweiten E-Mail oder einer Nachricht im Kundenkonto bestätigt wurde.[23]

---

18 https://www.heise.de/security/meldung/BlueBorne-Bluetooth-Schwachstellen-auch-in-Amazon-Echo-und-Google-Home-3891500.html (zuletzt abgerufen: 11/2018).

19 Brunotte, CR 2017, S. 583, 586.

20 Heidrich/Maekler, c’t 22/2017, S. 87.

21 https://www.amazon.de/gp/help/customer/display.html?nodeId=201602230 (zuletzt abgerufen: 11/2018); https://www.amazon.de/gp/help/customer/display.html/ref=footer_cou?ie=UTF8&nodeId=505048 (zuletzt abgerufen: 11/2018).

22 Brunotte, CR 2017, S. 583, 586.

23 Siehe Fn. 21.

1. Alexa, informier mich!

Im Fernabsatz, das heißt bei Verträgen bei denen für den Vertragsschluss ausschließlich Fernkommunikationsmittel – zu denen auch internetbasierte Sprachassistenten zählen – sowohl vom Verbraucher als auch vom Unternehmer verwendet werden (§ 312c Abs. 2 BGB), müssen grundsätzlich umfangreiche Informationspflichten beachtet werden. Diese finden sich insbesondere in § 5a Abs. 2, Abs. 3 UWG und §§ 312d, 312i und 312j BGB.[24]

Nach § 5a Abs. 2 S. 2 Nr. 2, Abs. 3 Nr. 1-5 UWG sind daher zum Beispiel die Merkmale der zu bestellenden Ware, Identität und Anschrift des Unternehmers, Preis, Versandkosten, Zahlungs-, Liefer- und Leistungsbedingungen, der Beschwerdeweg und das Recht zum Rücktritt oder Widerruf durch den Sprachassistenten bereits vor Einlegen des Kaufgegenstandes in den virtuellen Warenkorb zu nennen. Es ist offensichtlich, dass diese Fülle an Informationen einen bequemen und schnellen Spracheinkauf verhindert. Zudem haben Sprachassistenten in der Regel kein oder nur ein kleines Display, sodass dem Nutzer die Informationen nicht oder nur umständlich angezeigt werden können. Diesem Manko mit einem Verweis auf eine App oder dem Webshop zu begegnen scheitert an den Vorgaben des EuGH und des BGH, die ein Ausweichen auf andere Medien erst erlauben, wenn es unmöglich ist, die bereitzustellenden Verbraucherinformationen im gewählten Medium darzustellen.[25] Sprachassistenten können die Informationen aber wiedergeben, sodass die Übermittlung nicht unmöglich ist.

Dass das vorstehende Vorgehen unzulänglich ist – wer will schon seitenlange Erklärungen vorgelesen bekommen –, hat auch der Gesetzgeber erkannt und erleichterte Informationspflichten zugelassen. Diese gelten gemäß § 312d Abs. 1 S. 1 BGB i.V.m. Art. 246a § 3 EGBGB auch für sprachgesteuerte digitale Assistenten.[26] Hiernach müssen nur noch die Kerninformationen nach Art. 246a § 3 EGBGB wie Ware, Gesamtpreis,

---

24 Koch/Schmidt-Hern, WRP 2018, S. 671, 673.

25 Koch/Schmidt-Hern, WRP 2018, S. 671, 674.

26 Busch, in: Gsell/Krüger/Lorenz/Reymann, beck-online.GROSSKOMMENTAR, Art. 246a, § 3 EGBGB, Rn. 5.1.

Identität des Unternehmers und das Widerrufsrecht mitgeteilt werden. Doch auch diese reduzierten Informationspflichten sind noch ein merkliches Hindernis während des Sprachkaufs, weshalb abzuwarten bleibt, ob die Verbraucher dies tolerieren.

2. Wenn Alexa fremdgeht!?

Losgelöst von der Problematik der Informationspflichten stellt sich weitergehend die Frage, was eigentlich passiert, wenn nicht der Besitzer selbst einen Einkauf tätigt, sondern sein Kind, ein Besucher oder gar der Moderator im Fernsehen? Man könnte zum einen davon ausgehen, dass der Inhaber des automatisiert agierenden Sprachassistenten bei Inbetriebnahme des Geräts generell jede an den Assistenten übermittelte Erklärung als seine eigene Willenserklärung gelten lassen will.[27] Diese umfassende Annahme entspricht aber sicherlich nicht dem Willen des Nutzers, vielmehr möchte dieser darüber wachen, welche Einkäufe über seinen Assistenten getätigt werden. Dem Rechnung tragend wäre wegen der Haftung des Vertreters ohne Vertretungsmacht nach § 179 Abs. 1 BGB, welcher auch das Kind oder der Moderator sein könnten, an eine Lösung über das Stellvertretungsrecht zu denken. Dies scheitert bei Minderjährigen aber am Haftungsausschluss nach § 179 Abs. 3 BGB und beim Nachrichtensprecher am fehlenden Erklärungsbewusstsein.[28] Letzterer kann nicht erkennen, dass seine Aussage in allen Haushalten, die gerade die Nachrichten schauen, Alexa auslöst. Danach läge das Kontrahierungsrisiko allein beim Vertragspartner (exemplarisch: Amazon).

Wie man es dreht und wendet, jede der beiden Lösungen erscheint unbillig, weshalb ein Regulierungsbedürfnis in dieser Frage besteht. Abhilfe könnte ein Einwilligungserfordernis schaffen.[29] Ein solches offeriert auch Amazon. Der Sprachkauf über Alexa kann bei Hinterlegung eines 4-stelligen Bestätigungscodes ohne dessen Aussprache nicht abgeschlossen werden.[30] Das Einwilligungserfordernis macht den Sprachkauf sicherer

---

27 Specht/Herold, MMR 2018, S. 40, 42.

28 Specht/Herold, MMR 2018, S. 40, 42.

29 Specht/Herold, MMR 2018, S. 40, 42.

30 https://www.amazon.de/gp/help/customer/display.html?nodeId=201952610 (zuletzt abgerufen: 11/2018).

aber eben auch nur sicherer. Denn bestellt beispielsweise ein Dritter unautorisiert mit dem Code des Besuchten über dessen Sprachassistenten Produkte, liegt ein Handeln unter fremdem Namen vor.[31] Nach den entsprechend anzuwendenden Regeln über die Stellvertretung, §§ 164 ff. BGB, bindet eine solche Bestellung zunächst den Geräteinhaber. Sodann hängt es davon ab, ob der Geräteinhaber wusste oder hätte wissen können, dass Dritte seinen Bestätigungscode kennen. War dem so, liegt eine Duldungsvollmacht vor und er haftet voll.[32] Andernfalls haftet der Dritte nach § 179 Abs. 1 BGB.

Der freigeschaltete Sprachkauf bietet demnach aufgrund seiner technischen Ausgestaltung ein zusätzliches Haftungsrisiko für den registrierten Inhaber.

V. Alexa, was hast du angerichtet?

Die Konsequenzen (un-)bewusster Einkäufe durch Dritte über Sprachassistenten dürften sich zumeist im privaten Bereich in Anbetracht des Verbraucherwiderrufs gemäß §§ 355 ff. BGB in Grenzen halten. Was aber, wenn beispielsweise Alexa sich verhört und reagiert, obwohl dies eigentlich gar nicht angezeigt wäre und dadurch stört oder gar einen (irreparablen) Sach- oder Personenschaden verursacht? Sei nur an ein vergessenes Bügeleisen an einer von ihr gesteuerten Steckdose gedacht, das einen Wohnungsbrand entfacht. Wer haftet dann?

Diese Frage stellte sich auch Oliver H. als die Polizei ihm die Kosten für den Schlüsseldienst zwecks Öffnung seiner Wohnungstür nach nächtlicher Ruhestörung in Rechnung stellte.[33] Alexa hatte in seiner Abwesenheit infolge eines Fernzugriffs lautstark Musik gespielt.[34]

Diese Beispiele zeigen die Relevanz der Problematik.

---

31 Säcker et al./Schubert, § 164, Rn. 144.

32 Heidrich/Maekler, c't 22/2017, S. 86, 87.

33 http://www.sueddeutsche.de/panorama/sprachassistent-alexa-feiert-alleine-party-bis-die-polizei-kommt-1.3737128?reduced=true (zuletzt abgerufen: 11/2018).

34 http://www.sueddeutsche.de/panorama/sprachassistent-alexa-feiert-alleine-party-bis-die-polizei-kommt-1.3737128?reduced=true (zuletzt abgerufen: 11/2018).

1. Der Assistent, der Entwickler oder ich?

Im Rahmen der Haftung für Fehlverhalten intelligenter Assistenten dreht sich alles um die Frage wem dieses zuzurechnen ist, wenn es keiner natürlichen oder juristischen Person zuzuordnen ist.[35] Eine Haftung des Nutzers eines Sprachassistenten infolge Verschuldens nach § 823 Abs. 1 BGB scheitert zumeist daran, dass dieser bei der Überwachung der Reaktion des Assistenten seine Verkehrssicherungspflicht beobachtet hat und für ihn im Übrigen die fehlerhafte Reaktion auch nicht vorhersehbar war. Hieran anknüpfend wird derzeit in der Rechtswissenschaft intensiv die Frage diskutiert, ob der Nutzer verschuldensunabhängig vergleichbar dem Halter eines Fahrzeuges (§ 7 StVG) oder eines Tieres (§ 833 StGB) haften muss.

2. Die E-Person

Losgelöst von dem vorstehenden Versuch die Frage der Zurechnung in Anlehnung an das bestehende Recht zu lösen warf zuletzt das EU-Parlament die Frage auf, ob neben natürlichen und juristischen Personen Maschinen eine eigene Rechtsfähigkeit erhalten sollten.[36] Da diese naturgemäß über kein Vermögen verfügen, bedürfte es wohl eines Haftungsfonds für Roboter oder einer Versicherungspflicht,[37] damit Ansprüche gegen sie sinnvoll geltend gemacht werden könnten.
Das Ergebnis der Diskussion über die Haftung autonomer Systeme ist noch völlig offen. Der Regulierungsbedarf in dieser Frage folgt aber aus dem wohl unaufhaltsamen Aufstieg intelligenter Assistenten. Im obigen

---

35 Börding et al., CR 2017, S. 134, 140.

36 Europäisches Parlament, Zivilrechtliche Regelungen im Bereich Robotik, Entschließung des Europäischen Parlaments vom 16. Februar 2017 mit Empfehlungen an die Kommission zu zivilrechtlichen Regelungen im Bereich Robotik, (2015/2103(INL)) – P8_TA(2017)0051.

37 Borges, NJW 2018, S. 977, 980.

Fall der Party mit Alexa hatte Oliver H. Glück und Amazon kam trotz uneindeutiger Rechtslage nachdem das Ereignis viral ging für die Kosten des Schlüsseldienstes auf.

VI. Was ist das neue Normal? Ist es wünschenswert? Wer dürfte die Vorherrschaft erlangen?

Wer heutzutage einen Amazon EchoDot sein eigen nennt, darüber hinaus Amazon-Prime-Mitglied ist und entweder in den Großstädten München, Berlin, Potsdam oder Hamburg lebt, für den könnte bereits normal sein, was für andere erst noch zum neuen Normal werden dürfte. Ist der Kühlschrank leer, füllt Alexa ihn auf Zuruf bis 23:00 Uhr am Vorabend via AmazonFresh am Folgetag in einem frei zu wählenden 2h-Fenster wieder auf.[38] Diese Liefereigenschaft dürfte Alexa zur vorherrschenden digitalen Plattform der Zukunft machen, denn lästiges Tütenschleppen und Schlangen an der Kasse entfallen.[39] Dass Amazon mit Alexa derzeit auf dem Vormarsch ist, zeigt sich auch an dem Umfang, den die Berichterstattung über sie in diesem Beitrag erfordert.

1. Auswirkungen

Doch welche Auswirkungen gehen mit diesem wohl künftigen Wandel des Konsumverhaltens einher? Jeder, der Alexa auffordert, etwas zu bestellen, möchte keinen langen Dialog mit ihr darüber führen, was sie genau bestellt. Vollmilch ist Vollmilch, ein roter süßer Apfel ist ein roter süßer Apfel und ein weißes T-Shirt mit V-Ausschnitt ist ein weißes T-Shirt mit V-Ausschnitt. Damit der Bestellprozess, also der Dialog mit Alexa, der ohnehin wegen der Informationspflichten schon eine gewisse Länge hat, einfach ist, dürfte Amazon beispielsweise nur eine Vollmilch-Marke anbieten, was zu einem Verlust der Markenvielfalt und einer neuen Monopolstellung gegenüber den Produzenten führen könnte.[40] Selbst wenn zu

---

38 https://www.amazon.de/gp/help/customer/display.html?nodeId=202071690 (zuletzt abgerufen: 11/2018).

39 Klotz, S. 13.

40 Klotz, S. 13.

einem Produkt mehrere Auswahlmöglichkeiten bestünden, so muss davon ausgegangen werden, dass Amazon vorrangig das meist-verkaufte Produkt oder dasjenige eines Partners durch Alexa auswählen lässt.[41] Dies dürfte kleine Händler benachteiligen. Diese mitunter für zahlreiche heutige Marktteilnehmer existenzielle Zukunftsfrage steht auch bereits wegen ihrer kartellrechtlichen Relevanz im Fokus des Bundeskartellamts, wie dessen Präsident im vergangen Jahr verlauten ließ.[42] Weiterhin dürfte durch das sich verändernde Konsumverhalten der bargeldlose Zahlungsverkehr gegenüber dem Bargeschäft Zahlungsstandard werden und der Lieferverkehr in den Innenstädten einen neuerlichen Höchststand erreichen.

2. Eigentlich unerwünschte Effekte

Diese Auswirkungen sind eigentlich nicht im gesellschaftlichen Sinne. Dem Verlust an Vielfalt und dem sich wohl abzeichnenden Verlust an Arbeitsplätzen steht allein ein Mehr an Komfort gegenüber. Zwar entstehen auch Arbeitsplätze im Zusammenhang mit der digitalen Assistenz, diese sind aber zumeist gerade im Bereich der Zustellung oftmals weniger gut bezahlt.

Sprachassistenten eröffnen einen 24/7-Zugang zum Nutzer, womit derjenige, der über diese Schnittstelle wacht, in zuvor nie dagewesener Weise Kontrolle über die Inhalte – beispielsweise Nachrichten – hat, die den Nutzer erreichen. Insoweit dürfte logische Konsequenz sein, dass Anbieter über den neuen Zugang zum Nutzer zukünftig auch Werbung präsentieren und zu kostenpflichtigen Angeboten leiten.[43]

VII. Wo geht die Reise hin?

Seit der Erfindung der Dampfmaschine und der sich anschließenden Industrialisierung, Automatisierung und nun Digitalisierung ist die Verzahnung von Mensch und Maschine immer enger geworden. Mit der Sprachsteuerung von Maschinen steht offensichtlich das nächste Level in dieser

---

41 Klotz, S. 13.

42 MMR-Aktuell 2017, 393376.

43 Bager, c't 22/2017, S. 64, 69.

schon langen und erfolgreichen Entwicklungsstory an. Brachte einst die Fernbedienung neue zuvor ungeahnte komfortable Bedienmöglichkeiten, so verheißt die Sprachsteuerung mit dem Alles-und-zu-jeder-Zeit-auf-Zuruf nun noch viel Größeres. Schon jetzt erleben wir den Run der Tech-Giganten um technologische Überlegenheit, Geschwindigkeit und Image.[44] Die Schnittstelle zwischen Mensch und Maschine ist einer der zukünftig bedeutendsten Machtfaktoren.

1. Alexa überall und immer

Neben den Sprachassistenten in Smartphones, die schon seit längerem über ein Display verfügen, werden mehr und mehr auch die stationären Assistenten mit solchen ausgestattet. Hierüber ergibt sich künftig ein weiterer Zuwachs an Fähigkeiten. Mit dem in den USA vertriebenen Amazon Echo Look ist es schon heute möglich, dass Künstliche Intelligenz den Look seines Anwenders bewertet. Computerunterstützte Realitätswahrnehmung, sog. Augmented Reality, führt heutzutage wie im Beispiel des Amazon Echo Look meist nur zur Ergänzung von Bildern oder Videos mit computergenerierten Zusatzinformationen durch Einblendungen.[45] Stellt man sich aber eine Brille vor, mit der man sprechen kann, die auf Befehle reagiert und die Antworten via Knochenschall zurückgibt, kann man aber erahnen welches Potential noch vor uns liegt.[46] Denn im Vergleich zur bisher nicht wirklich zum Durchbruch gelangten Brille Google Glas, erscheint die Vorstellung einer Brille nur mit Sprachsteuerung real.

Neben der gegenständlichen Weiterentwicklung der Sprachassistenz durch den Einbau in weitere Geräte wird vor allem auch die Software weiter zulegen. Entgegen dem geschlossenen System von Apple hinter dem Assistenten Siri, bieten offene Systeme wie die Plattform hinter Amazons Alexa jedem Drittanbieter die Möglichkeit für den Sprachassistenten weitere Fähigkeiten (im Falle von Alexa sog. Skills) zu entwickeln und zu

---

44 Thomas, „Hallo, Computer!“.

45 https://de.wikipedia.org/wiki/Erweiterte_Realit%C3%A4t (zuletzt abgerufen: 11/2018).

46 Jurran, c’t 22/2017, S. 70, 72.

implementieren. Letzteres hat bereits zu zahlreichen Entwicklungen in diesem Bereich geführt.

2. Alexa verantwortungsbewusst

Neben dem reichhaltigen Zuwachs an Hard- und Software im Bereich der Sprachassistenz bleibt die Challenge gesellschaftlichen Herausforderungen adäquat zu begegnen. Insoweit gilt es für die Entwickler bei der Fortentwicklung der Sprachassistenten, diesen politische Neutralität zu implementieren und Rassismus und Sexismus entschlossen zu begegnen.[47]

VIII. Fazit

Der Siegeszug der Sprache als neues Medium der schnellen und effektiven Informationsübermittlung zwischen Mensch und Maschine über das Internet ist nicht mehr aufzuhalten. Mehr und mehr Bereiche des täglichen Lebens werden von intelligenten und smarten Sprachassistenten erobert. Damit ergeben sich laufend neue (rechtliche) Fragen, die ein kontinuierliches Monitoring zwecks Regulierung erfordern. En vogue ist derzeit die Frage des Datenschutzes. Mit der DS-GVO ist das Schutzniveau gestiegen. Aufgrund dessen sollte aber kein falsches Sicherheitsgefühl aufkommen. Sprachassistenten ist das jederzeitige Lauschen als auch eine fortwährende Internetverbindung immanent. Dies bietet Missbrauchspotential. Allein ist man im Zweifel nur bei Deaktivierung. Eine Revolution des Shoppings via Sprachsteuerung kann es nur geben, wenn die Bequemlichkeit über die Informationspflichten beim Vertragsschluss obsiegt. Neben der Klärung dieses Umstandes ist die Regelung der Haftung bei Fehlverhalten des Assistenten für den weiteren Erfolg dieser neuen Technologie unumgänglich. Ungeachtet der vorstehenden Unwägbarkeiten bietet die Sprachassistenz vor allem aber ein neues Level an Komfort insbesondere bei der Steuerung des Smart Home, was nicht nur älteren Menschen sehr entgegen kommt. Hiernach ist eins sicher: Im Bereich Sprachassistenz bleibt es spannend!

---

47 http://www.zeit.de/digital/internet/2018-01/sprachassistenten-alexa-sexismus-feminismus-sprachsteuerung-ki/komplettansicht (zuletzt abgerufen: 11/2018).

Literaturnachweise

Bager, Sprachassistenten: Die neue Bedienoberfläche, c't magazin für computertechnik 2017, Heft 22, S. 64-69.

bfbdi.bund.de, Datenschutz kompakt: Sprachassistenten., https://www.bfdi.bund.de/SharedDocs/Publikationen/DatenschutzKompaktBlaetter/Sprachassistenten.html?cms_templateQueryString=sprachassistenten&cms_sortOrder=score+desc (zuletzt abgerufen: 11/2018).

Börding et al., Neue Herausforderungen der Digitalisierung für das deutsche Zivilrecht, CR 2017, S. 134-140.

Borges, Rechtliche Rahmenbedingungen für autonome Systeme, NJW 2018, S. 977-982.

Brunotte, Virtuelle Assistenten – Digitale Helfer in der Kundenkommunikation, CR 2017, S. 583-589.

bundesnetzagentur.de, Bundesnetzagentur zieht Kinderpuppe „Cayla" aus dem Verkehr, https://www.bundesnetzagentur.de/SharedDocs/Pressemitteilungen/DE/2017/14012017_cayla.html;jsessionid=6D0157245ABD2594236EC56A4780DF12?nn=690686 (zuletzt abgerufen: 11/2018).

Busch, Erleichterte Informationspflichten bei begrenzter Darstellungsmöglichkeit, in: beck-online. GROSSKOMENTAR.

Europäisches Parlament, Zivilrechtliche Regelungen im Bereich Robotik, Entschließung des Europäischen Parlaments vom 16. Februar 2017 mit Empfehlungen an die Kommission zu zivilrechtlichen Regelungen im Bereich Robotik (2015/2103(INL)) – P8_TA(2017)0051.

Heidrich/Maekler, Alexa, darfst du das?, c't magazin für computertechnik 2017, Heft 22, S. 86-87.

Jurran, Feste Partnerin. Wie Alexa künftig in alle Lebensbereiche vordringt. , c't magazin für computertechnik, Heft 22, S. 70-73.

Klotz, Wie Sprachassistenten das Einkaufen verändern, http://www.digitalpublishingreport.de/dpr_Heft8_2017.pdf (zuletzt abgerufen: 11/2018).

Koch/Schmidt-Hern, Alexa, wo bitte geht es hier zum BGH?, WRP 2018, S. 671-676.

MMR-Aktuell, BKartA: Probleme im Online-Handel, MMR-Aktuell 2017, 393376.

Säcker et al., Münchener Kommentar zum BGB, Band 1, 7. Auflage München 2015.

Schantz/Wolff, Das neue Datenschutzrecht. Datenschutz-Grundverordnung und Bundesdatenschutzgesetz in der Praxis, München 2017.

Specht/Herold, Roboter als Vertragspartner?, MMR 2018, S. 40-44.

Thomas, „Hallo, Computer!“ Intelligente Spracherkennung kombiniert mit künstlicher Intelligenz markiert den Beginn einer neuen technologischen Ära. Wer wird am Ende das Sagen haben?, https://berlinvalley.com/spracherkennung/ (zuletzt abgerufen: 11/2018).

Verbraucherzentrale, Reaktions-Check: Alexa reagiert nicht nur aufs (Signal-)Wort, https://www.verbraucherzentrale.nrw/sites/default/files/2017-12/17-12-20_PM_Spracherkennung.pdf (zuletzt abgerufen: 11/2018).

L. Smart Home (Maurice Niehoff)

Stand: Mai 2018

Abstract: Smart Home

Der Begriff Smart Home stellt den Oberbegriff für die Vernetzung von technischen Geräten innerhalb einer Wohnung zur Optimierung des Wohnbereichs dar. Durch das Smart Home kann die Wohnung – Lebensmittelpunkt der meisten Menschen – erheblich an die Bedürfnisse der Bewohner angepasst werden. Dies steigert die Lebensqualität. Andererseits birgt das Smart Home durch die massenhafte Aufzeichnung und Verarbeitung von Daten nicht zu unterschätzende Risiken. Der vorliegende Beitrag skizziert die Funktionsweise und die Einsatzbereiche eines Smart Homes, stellt Vorteile und Risiken gegenüber und gibt einen Ausblick über mögliche Entwicklungen.

I. Einleitung

„Smart Home", „Smart Building", „Smartes Wohnen", „Smart Living". All' diese synonym verwendeten Begriffe kennzeichnen ein technisches Verfahren, welches in der Welt der zunehmenden Digitalisierung an Bedeutung gewinnt.

Gemeint ist hiermit die Vernetzung diverser technischer Geräte zur Optimierung des privaten Wohnbereichs. Sicherheitstechnik, Haushaltsgegenstände und Multimediageräte werden miteinander vernetzt, interagieren untereinander und sind zentral steuerbar.[1] Ziel ist die optimale Gestaltung des räumlichen Umfeldes. Schließlich ist die Wohnung primärer Rückzugsort und Lebensmittelpunkt der meisten Menschen. Das Smart Home passt sich somit den Bedürfnissen und Gewohnheiten seiner Be-

1 Schiller, Was ist ein Smart Home? Geräte und Systeme.

wohner an, um eine Erhöhung der Wohn – und Lebensqualität zu erreichen.[2] Von Sicherheitskameras, über Licht – und Energiesteuerung, zu Saugrobotern und vernetzen Kühlschränken. Der Fantasie des Smart Homes sind im „Internet der Dinge“[3] diesbezüglich keine Grenzen gesetzt.

Folgendes Beispiel ist längst keine Zukunftsmusik mehr:

P kommt von der Arbeit nach Hause. Vor seiner Haustür stehend, wählt sich sein Smartphone bereits in das heimische WLAN-Netz ein. Gleichzeitig erkennt die Sicherheitskamera an der Eingangstür eine Bewegung. Dank der Information des Smartphones weiß diese, dass es sich um den P handelt. Die Haustür öffnet sich. Der P macht es sich erstmal auf der Couch gemütlich.

Sein vollautomatischer Saugroboter war den Tag über schon fleißig und hat die Wohnung geputzt. Der ebenfalls vernetzte Kühlschrank hat die aufgebrauchten Vorräte selbst nachbestellt.

Es ist 20 Uhr. Der Smart-TV des P schaltet sich pünktlich ein und wechselt auf den Sender ARD – Tagesschau. Schließlich weiß sein kluger Fernseher, dass der P immer um 20 Uhr die Tagesschau guckt. Hierzu dimmt sein Smart Home die Lichtquellen auf eine angenehme Farbtemperatur von 2600 Kelvin, so wie der P es gerne mag.

Nach einiger Zeit ermittelt der Sensor im Wohnzimmer: Wenig Sauerstoff in der Luft. Er sendet die Information an die Fensterkontakte, welche sich öffnen und die Wohnung kurz durchlüften. Nach einer optimalen Stoßlüftung schaltet sich die Heizung wieder an und reguliert die Wohnungstemperatur auf 19,5°C, die Wohlfühltemperatur des P. Dies erkennt die Heizung anhand der smarten Uhr des P, die dessen Körperaktivitäten misst.

Es ist 22:30 Uhr, das Smart Home weiß: Schlafenszeit für P. Der P bestätigt dies durch einen Klick auf seinem Smartphone: „Schlafen gehen“. Das Smart Home setzt die nötigen Schritte in Gang. Fenster und Türen

---

2 Cimiano/Herlitz, NZM 2016, S. 409, 413.

3 Der Begriff des “Internets der Dinge” meint die Vernetzung von Alltagsgegenständen untereinander und mit dem Internet zur Erleichterung des menschlichen Alltags, so z.B.: Bullinger/Hompel, S.XIX, XXIII.

werden geschlossen, Alarmsystem aktiviert, die Heizung wird auf 18°C runtergestellt.

Morgen früh wird der P dann von seinem klugen Wecker schon um 6:23 Uhr geweckt. Denn dieser weiß, dass der P 22 Minuten im Stau stehen muss.

Im Jahr 2017 lag die Anzahl an mit Smart-Home-Funktionen ausgestatteten Privathaushalten in Deutschland bei 4,5 Millionen, was einen Anteil von 11,7 Prozent bedeutet.[4] Hierbei ist von einem Marktumsatzvolumen von ca. 1,8 Mrd. Euro auszugehen.[5]

Dieser Trend soll sich in den nächsten Jahren fortsetzen. So wird prognostiziert, dass sich die Anzahl der Smart-Home-Privathaushalte im Jahr 2020 auf 9,2 Mio. Haushalte verdoppelt hat.[6] Hierbei liegt der Fokus der aktuellen Nutzung auf dem Energiemanagement und dem Entertainment, welche jeweils von über 50 Prozent der Smart-Home-Nutzer angewendet werden.[7] Ein Hauptgrund der Nichtnutzer ist in den relativ teuren Anschaffungskosten zu sehen, welche ¾ der Befragten als Grund angaben.[8]

Dieser Beitrag soll dem Leser einen Überblick über die Thematik rund um das Thema Smart Home verschaffen.

Hierzu werden in einem ersten Schritt die verschiedenen Einsatzgebiete im Smart-Home-Bereich ausgebreitet (II.).

Daran anschließend wird dessen Funktionsweise erläutert (III.).

Danach wird die Verknüpfung zu Big Data geschaffen (IV.).

Aus der Verknüpfung werden die Vorteile und Risiken im Bereich des Smart Homes aufgeworfen (V.) und letztlich ein vorläufiges Fazit gezogen und ein Blick in die Zukunft gewagt (VI).

---

4 Statista, Digital Market Outlook 2017.

5 Statista, Digital Market Outlook 2017.

6 Statista, Digital Market Outlook 2017.

7 Splendid Research, Welche der folgenden Anwendungen aus dem Smart Home-Bereich nutzen Sie aktuell?.

8 Splendid Research, Welche der folgenden Anwendungen aus dem Smart Home-Bereich nutzen Sie aktuell?.

II. Einsatzbereiche im Smart Home

Um einen Eindruck und Überblick über die Spannweite von Smart-Home-Anwendungen zu gewinnen, werden die Smart-Home-Anwendungen in fünf Einsatzbereiche[9] aufgeteilt und beleuchtet.

1. Energiemanagement

Ein „Smart Meter“, also ein intelligenter Stromzähler, zeichnet das Energiemanagement in einem Smart Home aus.

Hauptziel ist die Senkung des Strombedarfs, welche durch die Novellierung des Energiewirtschaftsgesetzes gefördert wurde. So wurde z. B. § 21b Abs. 3a EnWG eingeführt, wonach eine Umstellung auf Smart Meter ermöglicht werden muss.[10]

Smart Meter zeichnen sich gegenüber herkömmlichen, mechanisch analogen Stromzählern dadurch aus, dass diese die Nutzungsdaten der Verbraucher digital aufzeichnen. Hierdurch wird der Verbrauchswert zum einen gespeichert, zum anderen werden diese Daten zur weiteren Verarbeitung und Kommunikation bereitgestellt. Verbraucher können nicht bloß einen Gesamtverbrauch ablesen, sondern ihre Verbrauchshistorie und ihr Benutzerverhalten einsehen, analysieren und so ihren individuellen Energieverbrauch optimieren.[11]

Das Smart Meter kann des Weiteren mit anderen Elektronikgeräten im Smart Home verbunden und Abläufe so optimiert werden. Zu denken ist zuerst an intelligente Heizungsthermostate, die anhand der Zählerinformationen das Benutzerverhalten der Verbraucher erkennen und die Heizungssteuerung an dieses gelernte Verhalten anpassen. Aber auch an eine Fernsteuerung per Smartphone ist beispielsweise zu denken.[12]

---

9 Eine Aufteilung in diese fünf Bereiche scheint die allgemeine Auffassung zu sein. So etwa in: Schulze-Sturm, S. 5 ff. oder in Splendid Research GmbH, Smart Home Monitor 2017.

10 ASUE Arbeitsgemeinschaft für sparsame und umweltfreundlichen Energieverbrauch e.V., S. 9.

11 ASUE Arbeitsgemeinschaft für sparsame und umweltfreundlichen Energieverbrauch e.V., S. 5; Kitzler, S. 15.

12 Wendel, Was sind smarte Thermostate und welche lohnen sich?.

Smart Meter dienen weiterhin der Schnittstelle zum Smart Grid, also einem intelligenten Stromnetz. Hierzu werden die gesammelten Informationen der Verbraucher an die Energieversorgungsunternehmen weitergeleitet. Diese können anhand der Informationen Optimierungen in der Energieversorgung vornehmen.[13]

Ein weiterer Anwendungsbereich sind etwa Leuchtmittel, die gekoppelt an bestimmte Ereignisse ein- oder ausgeschaltet werden oder ihre Farbe ändern.

2. Unterhaltungsmedien

Im Bereich der Unterhaltungsmedien hat vor allem das smarte TV-Gerät Einzug in die deutschen Haushalte erhalten. Im Jahr 2017 waren 31,9 Prozent mit einem solchen Gerät ausgestattet, Tendenz steigend.[14]

Ein Smart TV zeichnet sich gegenüber einem herkömmlichen TV-Gerät dadurch aus, dass es nicht bloßes Ausgabegerät ist. Vielmehr stellen die smarten TV-Geräte nichts anderes dar, als einen Computer mit tv-typischer Bedienweise.[15] Klassischer Anwendungsfall ist die Nutzung von Streamingdiensten über die Internetverbindung des TV-Gerätes.

Doch Smart TV ist nicht gleich Smart TV. Wirklich intelligent werden diese Systeme erst, wenn sie nicht bloß isoliert genutzt, sondern im Rahmen des Smart Homes mit weiteren Geräten verbunden werden. Zu denken ist hier zuallererst an Lautsprechersysteme, die das TV-Gerät zum Heimkino aufwerten. Aber auch eine Kombination mit der Zimmerbeleuchtung ist denkbar, die beim Anschauen eines Spielfilms automatisch die Beleuchtung, ähnlich einer Kinoatmosphäre, dimmt. Passend zum Genre des Films in unterschiedlichen Farbtemperaturen.

---

13 Detaillierte Informationen hierzu: von Schönfeld/Wehkamp, in: Hoeren/Kolany-Raiser (Hrsg.), Big Data zwischen Kausalität und Korrelation, S. 108-126.

14 ALM. (n.d.), Anteil der TV-Haushalte in Deutschland mit internetfähigem Fernsehgerät (Smart-TV) im Haushalt in den Jahren 2013 bis 2017.

15 Schiller, Was ist ein Smart TV? – Informationen, Erklärung und Anbieter.

3. Haushaltsgeräte

Gerade im Bereich der klassischen Haushaltsgeräte sind unzählige Formen und Kombinationen zur Smart-Home-Nutzung denkbar.

Alle diese Kombinationen dienen der Steigerung des Komforts. Aus diesem Grund sind die smarten Haushaltsgeräte mit einem Volumen von knapp 360 Mio. Euro der umsatzstärkste Markt.[16]

Führend ist zurzeit der Einsatz von smarten:

Kühlschränken

Waschmaschinen

Saugrobotern

Rasenmähern

So verfügen smarte Kühlschränke etwa über eine eingebaute Kamera, die es ermöglicht, aus dem Supermarkt zu überprüfen, welche Produkte im Kühlschrank fehlen. Die Waschmaschine schaltet sich passend dann ein, dass die Wäsche exakt nach Feierabend zum Trocknen bereit steht. Auch der Saugroboter beginnt erst dann seine Arbeit, wenn die Bewohner aus dem Haus sind. Der Rasenmäher verrichtet seine Arbeit ebenso nur in den Zeiten, in denen der Rasen nicht genutzt wird.[17]

4. Sicherheit

Neben dem Komfort spielt auch die Sicherheit eine wichtige Rolle beim smarten Home.

So bieten Smart-Home-Anwendungen intelligente Überwachungssysteme an. Überwachungskameras, Schlösser, Tür- und Fenstersensoren werden vernetzt und verstärken somit die Zugangskontrollen gegenüber Einbrechern oder ungebetenen Gästen. So können etwa Sensoren an geschlossenen Fenstern und Türen erkennen, wenn sich ein Einbrecher

---

16 Statista, Digital Market Outlook 2017.

17 Schiller, Was ist ein Smart Home? Geräte und Systeme.

hieran zu schaffen macht. Es wird dann eine Information an den Hausbesitzer gesendet, Lichter zur Abschreckung eingeschaltet oder ein Alarmsignal ertönt.[18]

5. Gesundheit

Das derzeit noch geringste Marktvolumen von 40 Mio. Euro im Smart-Home-Bereich ist im Sektor Gesundheit anzusiedeln. Dem steht entgegen, dass es mit einem prognostizierten Wachstum von 60 Prozent das mit Abstand am stärksten wachsende Segment darstellt.[19]

Der Bereich des „Ambient Assisted Living“ (AAL) dient dazu, es älteren Menschen zu eröffnen, möglichst lange in ihrer gewohnten Umgebung zu leben. Die zu Deutsch genannten „altersgerechten Assistenzsysteme“ sollen die Selbstständigkeit und ein selbstbestimmtes Leben fördern.[20] Möglich gemacht wird dies durch smarte Geräte und Anwendungen in der (ambulanten) Pflege, Sicherheit, Kommunikation und der Haushaltsversorgung.[21] So wird die Haushaltsversorgung durch diverse smarte Geräte erleichtert, so z. B. der bereits dargestellte Saugroboter. Grundsätzlich zeichnen sich diese Geräte durch möglichst umfassende Automatikfunktionen aus, sodass keinerlei oder nur geringfügige Bedienungen benötigt werden. Sicherheitsaspekte werden gefördert durch Sensoren, welche im Notfall ein Signal an eine Notrufzentrale versenden. Exemplarisch zu nennen sind hier Sensoren an der Badewanne, die ein Überlaufen verhindern, aber auch Sensoren im Teppich, die einen Sturz erkennen sollen. Die Pflege kann unter anderem durch die Aufzeichnung der vitalen Daten gefördert werden, sowie durch eine Vernetzung mit dem ambulanten Pflegedienst.

III. Funktionsweise eines Smart Homes

Bei der Funktionsweise eines Smart Homes ist generell zwischen zwei verschiedenen Arten zu unterscheiden.

---

18 Schaper, S. 601.

19 Pohlmann, Chancen und Risiken von Smart Home.

20 Christiansen/Klötzer, VersMed 2015, S.130.

21 Einordnung der Anwendungsbereiche orientiert an Georgieff, S. 3.

Zentrale Systeme arbeiten mit einer zentralen Steuerungseinheit, einem sogenannten „Gateway“ oder auch „Hub“. Dieses ist das Herzstück des Smart Homes, Dreh – und Angelpunkt der smarten Geräte. Die smarten Geräte kommunizieren über das Gateway untereinander. [22]

Bei dezentralen Systemen erfolgt die Kommunikation der Geräte nicht über das zentrale Gateway, sondern unter den Geräten direkt.

Zu erörtern ist hierbei auch die Art der Interaktion zwischen den smarten Geräten, wobei zwischen dem IFTTT-Verfahren und dem „deep learning“-Prozess zu unterscheiden ist.

1. Zentrale Systeme

Die einzelnen smarten Geräte werden (vorzugsweise) kabellos mit dem Gateway verbunden.

Das Gateway dient als Sammel- und Verteilerstelle der ein- und ausgehenden Daten und ist somit eine Art Kommunikationszentrale. Anwender können darüber das Smart Home zentral steuern.[23]

Zur Verbindung mit dem Gateway dienen verschiedenste „Funksprachen“.[24] Neben den üblicherweise bekannten Formaten wie Bluetooth oder WLAN, wird im Smart-Home-Bereich vornehmlich auf effizientere Technologien zurückgegriffen. Zu nennen sind hier die Funktechnologien ZigBee, Z-Wave und EnOcean.[25] Diese Technologien zeichnen sich durch einen deutlich niedrigeren Energieverbrauch im Vergleich zur bekannten WLAN-Technologie bei deutlich weiterer Reichweite als die bekannte Bluetooth-Technologie aus. Sie sind daher weitaus besser geeignet für den Smart-Home-Bereich.[26]

Diese Vielfalt der Funkstandards führt zu der Problematik, dass das Gateway die Funkstandards der damit zu verbindenden smarten Geräte unterstützen muss. Um eine Inkompatibilität von Gateway und Endgeräten zu vermeiden, gibt es für die Verbraucher die Möglichkeit, geschlossene

---

22 Verbraucherzentrale, Smart Home – das „intelligente Zuhause“.

23 Schiller, Was ist ein Hub, Aufgabe, Funktion und Einsatzgebiete.

24 Schiller, Was ist ein Smart Home? Geräte und Systeme.

25 Jakobi et al., Das Zuhause smart machen – Erfahrungen aus Nutzersicht.

26 Ferrari-Herrmann, 5 wichtige Smart-Home-Standards.

Systeme zu erwerben. Hierbei handelt es sich um aufeinander abgestimmte Geräte eines Herstellers, welche allerdings nicht mit Geräten anderer Hersteller kompatibel sind.

Offene Systeme hingegen haben den Vorteil, dass Produkte verschiedener Hersteller miteinander kombiniert werden können. Allerdings muss dann die Kompatibilität von Gateway und den smarten Geräten beachtet werden.

Die Bedienung dieser Systeme erfolgt vornehmlich über das Smartphone, da dieses eine benutzerfreundliche und zeitgleiche effektive Bedienung ermöglicht. Das Smartphone wird zur „Fernbedienung des intelligenten Hauses“[27]. Aber auch eine endgerätlose Steuerung über Gestik und Sprachbefehle ist möglich.[28]

2. IFTTT und deep learning

Damit das Smart Home auch tatsächlich smart wird und nicht bloß eine Anhäufung von vernetzten technischen Geräten darstellt, bedarf es der Interaktion der verschiedenen smarten Geräte, einer sogenannten Maschine-Maschine-Kommunikation.[29]

Hierzu sind vor allem zwei Begriffe zu benennen:

Zum einen das „if-this-than-that“(IFTTT)-Verfahren und zum anderen das sogenannte deep learning.

a) IFTTT

Von einem „if-this-than-that“ Ablauf spricht man, wenn die smarten Geräte untereinander nach bestimmten Szenarien interagieren. So löst ein bestimmtes Ereignis (Gerät X wird angeschaltet/Temperatur erreicht X °C) eine vorher festgelegte Reihe anderer Ereignisse aus (Gerät Y wird angeschaltet, was dazu führt, dass Gerät Z ausgeschaltet wird). Beispielhaft ist das einleitende Szenario zu nennen: Das Ereignis „es ist 20 Uhr“ führt dazu, dass der Smart TV mit der Tagesschau eingeschaltet wird.

---

27 Schiller, Was ist ein Smart Home?.

28 Schiller, Was ist ein Smart Home?.

29 Skistims, S. 65.

Das Einschalten des Smart TV führt zur Dimmung des Lichts auf 2600 Kelvin.

b) deep learning

Über diese linearen, regelbasierten Konzepte hinaus, liegt der besondere Mehrwert von Smart Homes in der Selbstlernfunktion, dem deep learning.[30] Beim deep learning handelt es sich um die Fähigkeit des Systems, mitunter ohne jeglichen menschlichen Einfluss, Zusammenhänge und Strukturen zu erkennen, sich selbst zu hinterfragen und somit fortlaufend zu verbessern.[31] Diese Fähigkeit stellt auch die Basis für Künstliche Intelligenz dar. Als Basis dienen dem System die große Menge an erfassten Daten, die Big Data, welche als Trainingsdaten für das System fungieren.[32] So lernte im einleitenden Szenario das smarte Home anhand der Verhaltensweise des P, dass dieser regelmäßig um 20 Uhr die Tagesschau guckt und seine Wohlfühlfarbtemperatur 2600 Kelvin beträgt.

IV. Der Bezug zu Big Data

Damit das Smart Home möglichst effektiv und personalisiert arbeiten kann, benötigt es große Mengen an Daten, mithilfe derer es die Gewohnheiten und Vorlieben der Nutzer erlernen kann. In einem voll ausgestatteten Smart Home ist es daher keine Seltenheit, dass jeden Tag Datenmengen in Höhe von 100 Terabyte und mehr entstehen.[33] Dies entspricht der Größenordnung von 50-100 Festplatten.

Quellen dieser Datenmengen sind Aufzeichnungstechniken, die verschiedenste Wahrnehmungen erkennen und speichern. So nehmen etwa Kameras visuelle, Mikrophone auditive Informationen auf. Darüber hinaus können diverse Sensoren auch taktile sowie thermische Informationen verarbeiten. Auch jede Modifikation des Benutzers, also jede Einstellung, die dieser vornimmt, ist ein Input für das smarte Home.

---

30 Kreutzer/Land, S. 34.

31 Schmidhuber, Neural Networks 2015, S. 85, 86.

32 Schmidhuber, Neural Networks 2015, S. 85, 86.

33 Cimiano/Herlitz, NZM 2016, S. 409, 414.

V. Vorteile und Risiken

Die Verwendung von Smart-Home-Komponenten bietet viele Vorteile, birgt aber auch Risiken im tatsächlichen und rechtlichen Umfang, denen begegnet werden muss.

1. Vorteile

Vorteile eröffnen sich auf mehreren Ebenen. Zum einen sei hier genannt, dass das eigene Zuhause sich den eigenen Bedürfnissen mehr und mehr anpasst. Dem Nutzer wird ein gesteigerter Komfort im Leben geboten. Darüber hinaus werden viele typische alltägliche Verrichtungsarbeiten durch das System automatisch erfüllt, ohne dass es eines Einflusses des Nutzers bedarf. Dies lässt Zeit für andere Dinge. Es wird also die persönliche Selbstbestimmung und Entfaltung eines Jeden gesteigert.[34]

Darüber hinaus bietet ein sinnvoll eingesetztes Smart Home auch große Möglichkeiten zur Steigerung des Gesundheitsschutzes und der Sicherheit. Man denke an das AAL, welches durch die altersgerechte Unterstützung zur Absicherung des selbstbestimmten Lebens beiträgt.[35] Aber auch die smarten Überwachungstechniken und Notrufsysteme können das smarte Home sicherer gegenüber ungebetenen Eindringlingen machen und somit die Privatsphäre verbessern.

Letztlich kann ein Smart Home auch zur Einsparung von Ressourcen dienen. So kann vor allem durch das Smart Meter und dem individuellen Energiemanagement eine deutliche Einsparung von Strom-, Wasser- und Gaskosten erzielt werden.

2. Risiken

Dem stehen aber nicht zu unterschätzende Risiken für die Nutzer entgegen. Die Erzeugung großer Mengen von besonders sensiblen, höchstpersönlichen Daten ruft vor allem den Datenschutz auf den Plan. Das Ziel eines Smart Homes, eine möglichst umfassende Aufzeichnung aller persönlichen Daten der Nutzer zu erfassen, widerstrebt den Grundzügen der

---

34 Skistims, S. 121, 123 f.

35 Christiansen/Klötzer, VersMed 2015, S. 130.

DS-GVO, welche ab dem 25.05.2018 gilt. Dies betrifft vor allem die umfassende Verarbeitung personenbezogener Daten im Sinne des Art. 4 Nr. 1 DS-GVO.

a) Zweckbindungsgrundsatz, Art. 5 Abs. 1 b) DS-GVO

Der Zweckbindungsgrundsatz besagt, dass personenbezogene Daten nur für bestimmte, eindeutig festgelegte Zwecke erhoben werden dürfen.[36] Dies ist bei Erfassung einzelner Komponenten im Smart Home nur schwer einzuhalten. Allzu oft wird es zu spontanen Zweckänderungen kommen.[37] Je nach eigenständiger Entwicklung der einzelnen Smart-Home-Komponenten werden die erfassten Daten für völlig verschiedene Zusammenhänge und Verarbeitungen genutzt. Dies wäre grundsätzlich gemäß Art. 5 Abs. 1 b) DS-GVO unzulässig und nur unter den Ausnahmevoraussetzungen aus Art. 6 Abs. 4 DS-GVO möglich.

b) Minimierungsgrundsatz, Art. 5 Abs. 1 c) DS-GVO

Der Grundsatz der Datenminimierung und Datensparsamkeit besagt, dass Datenverarbeitungsprozesse so konzipiert sein müssen, dass möglichst wenig personenbezogene Daten verarbeitet werden. Dies läuft der Arbeitsweise des Smart Homes, wie schon dargelegt, entgegen. Dessen Performance steigt gerade mit steigender Erzeugung und Verarbeitung von personenbezogenen Datenmengen.

c) Privacy by Design and by Default, Art. 25 DS-GVO

Zur Minimierung von personenbezogenen Daten schreibt die DS-GVO die Grundsätze des Privacy by Design und Privacy by Default in Art. 25 Abs. 1 und 2 DS-GVO vor. Dies bedeutet, dass Technik so eingerichtet sein muss, dass bereits durch die Konzeption der Technik und dessen Voreinstellung eine möglichst datenschutzfreundliche Ausgestaltung

---

36 Gola/Pötters, Art. 5, Rn. 12.

37 Geminn, DuD 2016, S. 575, 578.

sichergestellt ist.[38] Dies kann beispielsweise durch Pseudonymisierung, Löschpflichten und eine generelle Pflicht zur Datenminimierung erfolgen.[39]

d) Recht auf „Vergessenwerden", Art. 17 DS-GVO

Das Recht auf Löschung, auch „Recht auf Vergessenwerden" genannt, eröffnet den betroffenen Personen die Möglichkeit, vom Verwender von Daten unter bestimmten Voraussetzungen, die in Art. 17 Abs. 1 DS-GVO aufgelistet sind, zu verlangen, dass personenbezogene Daten gelöscht werden sollen. Dies ist etwa der Fall, wenn die betroffene Person die Einwilligung widerruft (lit. b) oder die Daten für den erhobenen Zweck nicht mehr notwendig sind (lit. a). Gerade hier sind Streitpunkte vorprogrammiert, nämlich darüber, wann im komplexen Gebilde eines Smart Homes mit mehreren, untereinander korrespondierenden Endgeräten und möglicherweise unterschiedlichen Verwendern Daten nicht mehr notwendig sind.

e) Recht auf Datenportabilität, Art. 20 DS-GVO

Das Recht auf Datenportabilität soll betroffenen Personen erleichtern, zwischen unterschiedlichen Anbietern zu wechseln, indem den betroffenen Personen die Daten in „einem strukturierten, gängigen und maschinenlesbaren Format" zur Verfügung gestellt werden sollen.[40] Dies ermöglicht, dass die betroffene Person ohne größeren Aufwand zwischen verschiedenen Anbietern wechseln kann und nicht wegen der technischen Hürde bei seinem Ausgangsanbieter bleibt.[41] Gedacht war dies ursprünglich für Kommunikationsclients und soziale Netzwerke, anhand der Voraussetzungen in Art. 20 Abs. 1 DS-GVO ist die Norm jedoch weitreichend anzuwenden. Im Rahmen des Smart Home dürfte dies zu praktischen Problemen führen. Es ist fraglich, inwiefern es den Anbietern von Smart-Home-Komponenten bei offenen Systemen technisch möglich ist,

---

38 Schantz, NJW 2016, S. 1841, 1846.

39 Paal/Pauly/Martini, Art. 25, Rn. 29-31.

40 Schantz/Wolff, Rn. 1237.

41 Schantz/Wolff, Rn. 1237.

den betroffenen Personen die Daten in der Form zur Verfügung zu stellen, dass diese Person die Daten auch – im Sinne der Vorschrift – nutzen kann. Dann nämlich müssten die Daten so zur Verfügung gestellt werden, dass die Daten des einen Anbieters vom anderen Anbieter genutzt werden können. Dies führt neben technischen Hürden auch zu Kollisionen in den Geschäftsgeheimnissen der Anbieter.

f) Cybercrime

Beim Smart Home handelt es sich um ein informationstechnisches System wie jedes andere auch. Dies bedeutet, dass es angreifbar ist und stellt gerade beim Smart Home besonders erhebliche Eingriffe in die Privatsphäre der betroffenen Personen dar, da hier sehr viele und sehr sensible Daten aufgezeichnet werden. Dadurch, dass das Smart Home grundsätzlich mittels des Routers mit dem Internet und der Cloud verbunden sein wird, ist dieser ein potentieller Angriffspunkt. So sind etwa Hackereingriffe zur Abschöpfung der gewonnenen Daten denkbar.[42] Auch unerlaubte Zugriffe auf Mikrofone und Kameras könnten einen erheblichen Eingriff in den Bereich der Wohnung darstellen.

Es bedarf hier einer regelmäßigen Überprüfung und des Schließens von Sicherheitslücken. Eine Alternative wäre, das Smart Home offline zu betreiben, was – unter Verzicht gewisser Feature – möglich ist.

2. Digitale Bevormundung

Als sozial-ethischer Aspekt kann dem Smart Home vorgehalten werden, es behindere das eigene Denken bzw. mache dieses überflüssig. Das Smart Home übernimmt mehr und mehr alle täglichen Handgriffe des Bewohners, sodass dieser in seinen eigenen vier Wänden nicht mehr selbstständig nachdenken muss, sondern nur noch vor sich hinleben kann.

VI. Fazit

Das Smart Home stellt eine interessante, zukunftsträchtige Möglichkeit für jedermann dar.

---

42 Skistims, S. 142.

Noch steckt die Entwicklung eher in den Kinderschuhen, die Entwicklung wird aber in der Zukunft stark ansteigen. So soll sich die Zahl der Smart Homes im Jahr 2020 im Vergleich zum Jahr 2017 verdoppelt haben.[43]

Neben vielen Vorteilen, die das Leben in den eigenen vier Wänden bietet, sind den Menschen auch durchaus dessen Risiken bewusst.

Unter den Personen, die an Smart Home kein Interesse haben, nennen 50 Prozent Privatsphäre und 2/3 steigende Automatisierungsangst.[44]

Diese Angst ist sicherlich nicht ganz unbegründet. Nutzer sollten verbraucherschutzrechtlich und datenschutzrechtlich sensibel bleiben. Dennoch sollten sie technische Innovationen nicht durch überzogene Angst abweisen. Mit bedachtem und verantwortungsvollem Umgang lässt sich aus dieser aufstrebenden Technik enormer Nutzen ziehen.

Literaturnachweise

ABIDA, Big Data – Lösung oder Problem? Dokumentation und Analyse der Bürgerkonferenzen, http://www.uni-muenster.de/Jura.itm/hoeren/itm/wp-content/uploads/ABIDA_B%C3%BCrgerkonferenzen_Ergebnisbericht.pdf (zuletzt abgerufen: 11/2018).

ALM. (n.d.), Anteil der TV-Haushalte in Deutschland mit internetfähigem Fernsehgerät (Smart-TV) im Haushalt in den Jahren 2013 bis 2017, In: Statista – Das Statistik-Portal, https://de.statista.com/statistik/daten/studie/325527/umfrage/anteil-der-tv-haushalte-in-deutschland-mit-smart-tv/ (zuletzt abgerufen: 11/2018).

ASUE Arbeitsgemeinschaft für sparsame und umweltfreundlichen Energieverbrauch e.V., Smart Meter – intelligente Zähler, Essen 2011.

Bullinger/Hompel, Internet der Dinge, Berlin/Heidelberg 2007.

Christiansen/Klötzer, Ambient Assisted Living – Ein Überblick, VersMed 2015, S. 130-132.

---

43 So bereits Fn. 6.

44 Splendid Research GmbH, Warum haben Sie kein Interesse an der Nutzung von Smart Home-Anwendungen?.

Cimiano/Herlitz, „Smart Wohnen!“ Die „intelligente“ Wohnung und rechtserhebliche Erklärungen über „Mieterportale“, NZM 2016, S. 409-417.

Ferrari-Herrmann, 5 wichtige Smart-Home-Standards, https://www.androidpit.de/das-sind-die-wichtigsten-smart-home-standards (zuletzt abgerufen: 11/2018).

Geminn, Das Smart Home als Herausforderung für das Datenschutzrecht, DuD 2016, S. 575-580.

Georgieff, Ambient Assisted Living Marktpotentiale IT-unterstützter Pflege für ein selbstbestimmtes Altern, in: Fazit Forschung Schriftenreihe, Stuttgart 2008.

Gola, Datenschutz-Grundverordnung, München 2017.

Jakobi et al., Das Zuhause smart machen – Erfahrungen aus Nutzersicht, http://141.83.80.211:8080/xmlui/bitstream/handle/123456789/5004/Jakobi_etal_2016.pdf?sequence=1 (zuletzt abgerufen: 11/2018).

Kitzler, Smart Meter – Aufgaben, Fähigkeiten und Nutzen für das zukünftige Smart Grid, München 2013, https://www.eal.ei.tum.de/fileadmin/tueieal/www/courses/UEEML/lecture/2014-2015-W/HauptseminarAusarbeitung_Smart_Meter.pdf (zuletzt abgerufen: 11/2018).

Kreutzer/Land, Digitale Markenführung – Digital Branding im Zeitalter des digitalen Darwinismus, Wiesbaden 2017.

Paal/Pauly, Datenschutz-Grundverordnung/Bundesdatenschutzgesetz, 2. Auflage München 2018.

Pohlmann, Chancen und Risiken von Smart Home, https://norbert-pohlmann.com/app/uploads/2017/10/334-Chancen-und-Risiken-von-Smart-Home-Prof.-Norbert-Pohlmann.pdf (zuletzt abgerufen: 11/2018).

Schantz, Die Datenschutz-Grundverordnung – Beginn einer neuen Zeitrechnung im Datenschutzrecht, NJW 2016, S. 1841-1847.

Schantz/Wolff, Das neue Datenschutzrecht, München 2017.

Schaper, Smart Home – eine Positionsbeschreibung, Wiesbaden 2016.

Schiller, Was ist ein Hub, Aufgabe, Funktion und Einsatzgebiete, https://www.homeandsmart.de/hub-smart-home-aufgabe-funktion-einsatzgebiete (zuletzt abgerufen: 11/2018).

Schiller, Was ist ein Smart Home? Geräte und Systeme, www.homeandsmart.de/was-ist-ein-smart-home (zuletzt abgerufen: 11/2018).

Schiller, Was ist ein Smart TV? – Informationen, Erklärung und Anbieter, https://www.homeandsmart.de/was-ist-ein-smart-tv (zuletzt abgerufen: 11/2018).

Schmidhuber, Deep learning in neural networks: An overview, Neural Networks 61 (2015), S. 85-117.

Schulze-Sturm, Blickwinkel Smart Home – Studien aus Angebots – und Nachfragesicht, in: Mittelstand-Digital, Ausgabe 4, Wissenschaft trifft Praxis, neue Formen des Home Experience Design, Begleitforschung Mittelstand-Digital, S. 5-11, Bad Honnef 2016.

Skistims, Smart Homes, Der elektronische Rechtsverkehr, Band 31 Baden-Baden 2016.

Splendid Research GmbH, Smart Home Monitor 2017, de.statista.com/outlook/279/137/smart-home/deutschland#market-revenue (zuletzt abgerufen: 11/2018).

Splendid Research GmbH, Warum haben Sie kein Interesse an der Nutzung von Smart Home-Anwendungen?, https://de.statista.com/statistik/daten/studie/757040/umfrage/fehlendes-interesse-an-smart-home-anwendungen-in-deutschland (zuletzt abgerufen: 11/2018).

Splendid Research GmbH, Welche der folgenden Anwendungen aus dem Smart Home-Bereich nutzen Sie aktuell?., https://de.statista.com/statistik/daten/studie/756909/umfrage/aktuelle-nutzung-von-smart-home-anwendungen-nach-kategorie-in-deutschland/., (zuletzt abgerufen: 11/2018).

Statista, Digital Market Outlook 2017, de.statista.com/outlook/279/137/smart-home/deutschland#market-revenue (zuletzt abgerufen: 11/2018).

Verbraucherzentrale, Smart Home – das „intelligente Zuhause“, https://www.verbraucherzentrale.de/wissen/umwelt-haushalt/wohnen/smart-home-das-intelligente-zuhause-6882 (zuletzt abgerufen: 11/2018).

Von Schönfeld/Wehkamp, Big Data & Smart Grid – Intelligente Energieversorgung zwischen Effizienz und Privatsphäre, in: Hoeren/Kolany-Raiser (Hrsg.), Big Data zwischen Kausalität und Korrelation, S. 108-126, Münster 2016.

Wendel, Was sind smarte Thermostate und welche lohnen sich?, https://www.homeandsmart.de/funktionen-smarter-thermostate (zuletzt abgerufen: *11/2018).*

M. Personalisierte Preise – Diskriminierung 2.0? (Tristan Julian Tillmann und Verena Vogt)

Stand: September 2018

Abstract: Personalisierte Preise – Diskriminierung 2.0?

Immer wieder geistern die Begriffe „personalisierte Preise“ oder „Preisdiskriminierung“ durch die Medien. So verwundert es nicht, dass sich eine regelrechte Phobie vor solchen Mechanismen in der Bevölkerung entwickelt hat. Zudem erscheint es so, als würde diese Technik der Preissetzung bereits verbreitet Anwendung finden. Aber worum handelt es sich dabei genau und in welchem Verhältnis stehen personalisierte Preise zu dynamischen Preisen? Der vorliegende Beitrag beantwortet diese Fragen und beleuchtet insbesondere die rechtlichen Aspekte von personalisierten Preisen.

I. Einleitung

Schon immer ist die Preisfindung, als zentrale Aufgabe eines jeden Händlers, verschiedenen Einflüssen unterworfen gewesen. Der endgültige Preis konnte jedoch nicht zuletzt durch das Verhandlungsgeschick des Käufers mitunter stark beeinflusst werden. Insofern war es lange Zeit nicht der Regelfall, dass bei einem Händler einheitliche Preise für alle Kunden galten.[1] Sowohl im Offline- als auch im Online-Handel findet nun schon seit längerem eine datengetriebene Personalisierung von Angeboten statt. Auf diese hat der Käufer, ob mit oder ohne Verhandlungsgeschick, keinen direkten Einfluss. Immer verstärkter tauchen individuelle Produktangebote, Gutscheine und Mitgliedschaftsvorteile auf. Durch die zunehmende Digitalisierung des Handels und den Einsatz von Big Data

[1] Obergfell, ZLR 2017, S. 290, 293; Wenglorz, S. 957; Reinartz et al., S. 3; Genth, Wirtschaftsdienst 2016, S. 863.

bekommen die Individualisierungsmöglichkeiten jedoch eine neue Dimension. Durch die Analyse der gesammelten Daten lassen sich Preise individuell in Echtzeit an die Preisbereitschaft des Kunden anpassen.[2] Gleichzeitig hat die Digitalisierung durch die Möglichkeit eines umfassenden Preisvergleichs, z. B. mittels Preissuchmaschinen, zu einer bis dato nicht bekannten Preistransparenz geführt.[3] Unternehmen sehen sich nun beim Einsatz personalisierter Preise mit neuen technischen, rechtlichen und gesellschaftlichen Herausforderungen konfrontiert.

II. Abgrenzung zu dynamischen Preisen

Im Gegensatz zu personalisierten Preisen sind dynamische Preise schon seit längerem bekannt. Dynamische Preise betreffen alle Konsumenten gleichermaßen und werden durch äußere Kriterien, wie zum Beispiel dem Wettbewerb der Unternehmer untereinander, der Beliebtheit des Produkts und dem Zeitpunkt der konkreten Nachfrage beeinflusst. Zu einem bestimmten Zeitpunkt gelten diese Preise für alle Kunden.[4] An diese Art von Preisschwankungen haben sich die Konsumenten bereits gewöhnt und sie akzeptiert.[5] Prominente Beispiele sind Benzin- und Reisepreise, insbesondere von Flügen, bei denen es regelmäßig zu erheblichen Preisschwankungen kommt.[6]

III. Ökonomische Aspekte

Mit personalisierten Preisen können aus Unternehmenssicht eine Vielzahl strategischer Ziele verfolgt werden. Neben der Gewinn- oder Umsatzsteigerung kann zum Beispiel auch Kundenbindung und -gewinn oder Markteintritt ein Ziel sein.[7] Wird eine Gewinn- oder Umsatzsteigerung verfolgt, ist das Ziel die Abschöpfung einer möglichst großen Konsumentenrente.[8]

---

2 Wenglorz, S. 958.

3 Genth, Wirtschaftsdienst 2016, S. 863, 867.

4 Schwaiger/Hufnagel, S. 10.

5 Obergfell, S. 292.

6 Wenglorz, S. 958.

7 Schwaiger/Hufnagel, S. 10; Reinartz et al., S. 18.

8 Zander-Hayat/Reisch/Steffen, VuR 2016, S. 403, 404.

Die Kunst besteht dann darin, die am Markt vorliegende heterogene Zahlungsbereitschaft zu nutzen, sodass ein Produkt viele verschiedene Preise für unterschiedliche Verbraucher zum selben Zeitpunkt hat.[9] Das heißt, dass im Ergebnis jeder genau den Preis zahlt, den er für das Produkt zu zahlen bereit ist. Das Abschöpfen der gesamten Konsumentenrente setzt eine entsprechende Marktmacht voraus.[10] Wahrscheinlicher ist, dass nur ein Teil dieser Konsumentenrente erzielt werden kann.

1. Bildung personalisierter Preise

Die Bildung personalisierter Preise erfolgt anhand verbraucherspezifischer Kriterien.[11] Dies können zum einen objektive Kriterien wie zum Beispiel das verwendete Endgerät, der Browser oder das Betriebssystem sein. Zum anderen können auch subjektive Kriterien wie das Alter, das Geschlecht, die Herkunft und das vorrausgegangene Surfverhalten des Verbrauchers Einfluss auf die Preisbildung haben.[12] Die objektiven und zumeist technischen Kriterien sind zwar einfach zu erfassen und auszuwerten, sie weisen jedoch nur eine geringe Aussagekraft in Bezug auf die Preisbereitschaft der Kunden auf.[13] Wesentlich interessanter für die Preisbildung sind die subjektiven Informationen über das bisherige Produktsuch- und Kaufverhalten des Verbrauchers.[14] Sofern ein Verbraucher in einem Onlineshop registriert ist, erfasst das entsprechende Unternehmen die bisherigen Produktsuchen sowie bisherigen Einkäufe und kann diese auswerten. Aber auch ohne Registrierung können beispielsweise durch den Einsatz von Trackingtools zahlreiche Informationen über den Kunden gesammelt werden.[15] Durch die Auswertung dieser Daten

---

9 Obergfell, ZLR 2017, S. 290, 293.

10 Schwaiger/Hufnagel, S. 22.

11 Zander-Hayat/Reisch/Steffen. VuR 2016, S. 403, 404.

12 Zander-Hayat/Reisch/Steffen, VuR 2016, S. 403, 404; Obergfell, ZLR 2017, S. 290, 293; Wenglorz, S. 960; Fezer/Büscher/Obergfell/Wenglorz, Rn. 81j.

13 Schleusener, S. 77.

14 Schleusener, S. 77; Miller, Journal of Technology Law & Policy, S. 41, 59.

15 Röttgen, in: Hoeren/Kolany-Raiser (Hrsg.), Big Data zwischen Kausalität und Korrelation, S. 84, 86/87.

kann eine Prognose über die Preisbereitschaft des jeweiligen Verbrauchers getroffen werden. Der Konsument erhält dann auf Basis dieser Prognose einen individuellen Preis.

2. Ökonomischer Nutzen und gesamtgesellschaftliche Wohlfahrt

In der Wissenschaft ist heftig umstritten, ob personalisierte Preise ökonomisch sinnvoll sind. Einige Stimmen gehen davon aus, dass personalisierte Preise den Wettbewerbsdruck erhöhen und der Profitabilität der Unternehmen schaden, während andere genau das Gegenteil erwarten.[16] Zudem wird davon ausgegangen, dass preissensible Kunden opportunistisch immer beim günstigsten Anbieter kaufen werden. Dadurch wird der Aufbau von langfristigen und profitablen Kundenbeziehungen beeinträchtigt.[17] In jedem Fall werden immer mehr Kunden aktiv nach verschiedenen Angeboten suchen, da sie sich nicht mehr darauf verlassen können, dass ihr Stammhändler ihnen einen attraktiven Preis bietet. Umso mehr Angebote dabei berücksichtigt werden müssen, umso größer ist die Wahrscheinlichkeit, dass von einem Kauf gänzlich abgesehen wird.[18] Positive Effekte können die Erschließung neuer Nachfragesegmente und die Stimulanz des Wettbewerbs durch personalisierte Rabatte sein.[19]

Der wohlfahrtsökonomische Nutzen ist ebenso schwer abzuschätzen. Könnten Unternehmen personalisierte Preise ohne Hindernisse durchsetzen, würden die Kunden schlechter gestellt werden. Die Unternehmen könnten die gesamte Konsumentenrente aller Kunden abschöpfen, ohne dass bei den Kunden etwas verbliebe.[20] Dieses Szenario ist jedoch auf-

---

16 Schwaiger/Hufnagel, S. 19/21.

17 Schwaiger/Hufnagel, S. 19.

18 Schwaiger/Hufnagel, S. 21; Kenning/Pohst, Wirtschaftsdienst 2016, S. 871, 872.

19 Obergfell, ZLR 2017, S. 290, 294.

20 Schwaiger/Hufnagel, S. 22; Tietjen/Flöter, GRUR-Prax 2017, S. 546; Schleusener/Hosell, S. 8; Schleusener, S. 80.

grund des zu erwarteten Kundenverhaltens und des Wettbewerbs unrealistisch.[21] Bei einem funktionierenden Wettbewerb bildet der Preis der Wettbewerber die Obergrenze für den eigenen Preis.[22] Aber selbst in diesem Fall werden die Verbrauchergruppen, die höhere Preise zu zahlen haben, Wohlfahrtseinbußen hinnehmen müssen.[23] Geht man davon aus, dass die Profitabilität der Unternehmen leidet, sei es weil der Wettbewerbsdruck steigt oder Kunden auf Käufe verzichten, führt dies zu sinkenden Preisen.[24] Dies kommt wiederum den Kunden zugute. Personalisierte Preise können jedoch auch direkt einen wohlfahrtsökonomischen Vorteil mit sich bringen. Die Erhöhung der Margen bei zahlungskräftigeren Kunden kann Umverteilungswirkungen haben.[25] Außerdem können, da jeder Kunde den seiner Zahlungsbereitschaft entsprechenden Preis bezahlt, auch einkommensschwache Verbraucher am Konsum teilnehmen.[26] Es wird jedoch befürchtet, dass die Gewinnmaximierungsinteressen der Unternehmen dazu führen, dass nur wirtschaftsstarken Kunden ein Preisvorteil eingeräumt wird, während die wirtschaftlich schwächeren und somit weniger attraktiven Kunden aus dem Markt gedrängt werden.[27] Benachteiligt werden könnten, neben Kunden mit einer schwachen Zahlungsbereitschaft, auch Kunden, die ein hohes Datenschutzbedürfnis haben oder die schlicht nicht gläsern gegenüber dem Anbieter sein wollen.[28] Schutzbedürftig scheinen zudem Kunden zu sein, die hinsichtlich der

---

21 Schleusener/Hosell, S. 8; Miller, Journal of Technology Law and Policy 2014, S. 41, 57.

22 Schleusener, S. 80.

23 Verbraucherzentrale Bundesverband e.V., Personalisierte Preise, S. 5; Schleusener/Hosell, S. 6.

24 Schwaiger/Hufnagel, S. 22; Miller, Journal of Technology Law and Policy, S. 41, 63.

25 Reinartz et al., S. 17.

26 Reinartz et al., S. 17.

27 Obergfell, ZLR 2017, S. 290, 294/295; Zander-Hayat/Reisch/Steffen, VuR 2016, S. 403, 405; Miller, Journal of Technology Law and Policy, S. 41, 94; Verbraucherzentrale Bundesverband e.V., Personalisierte Preise, S. 5.

28 Obergfell, ZLR 2017, S. 290, 295.

neuen Technologien weniger versiert sind oder die ihr eigenes Verhalten immer wieder falsch einschätzen.[29]

3. Hürden

a) Technologie

Big-Data-Anwendungen befähigen Unternehmen, grundsätzlich eine Unmenge an Daten über ihre Kunden zu sammeln und auszuwerten. Die Zahlungsbereitschaft eines Kunden kann daher nun mit relativ geringem Aufwand prognostiziert werden.[30] Personalisierte Preise können nicht nur im Online-Handel eingesetzt werden, sondern eignen sich über Kundenkarten, Apps oder mobile Bezahlsysteme auch für den stationären Einzelhandel.[31] Die gesammelten Daten münden dort vor allem in personalisierten Coupons.[32] Jedoch bestehen weiterhin Hürden, die den großflächigen Einsatz personalisierter Preise beeinträchtigen.

Derzeit scheinen die Anbieter noch nicht das nötige Know-How zu haben, um personalisierte Preise flächendeckend einzusetzen.[33] Dass die grundsätzlichen technologischen Möglichkeiten bestehen, bedeutet nicht, dass die Händler auch Zugriff auf diese haben. Die derzeitigen Preissetzungsherausforderungen sind nach wie vor klassischer Natur.[34] Die Anwendung von personalisierten Preisen wird daher zunächst von größeren Unternehmen ausgehen, welche die entsprechenden Ressourcen haben, um das nötige Know-How zu erwerben.[35] In technischer Hinsicht besteht beispielsweise das Problem, Kunden, die mehrere Endgeräte parallel nutzen, eindeutig zu identifizieren, da das Onlineprofil eines Kunden je nach Endgerät unterschiedlich ausfallen kann.[36] Um den Kunden jedoch nicht zu verärgern bzw. zu verwirren, sollte demselben Kunden immer

---

29 Reinartz et al., S. 17.

30 Schwaiger/Hufnagel, S. 10/11/42; Reisch et al., S. 21.

31 Schwaiger/Hufnagel, S. 12.

32 Schwaiger/Hufnagel, S. 12.

33 Schleusener/Hosell, S. 12; Reinartz et al., S. 8.

34 Reinartz et al., S. 8.

35 Schleusener, S. 76.

36 Schleusener, S. 77.

der gleiche Preis angezeigt werden.[37] Weiterhin muss bei der Analyse der Daten beachtet werden, dass ein Kunde auch unterschiedliche Preisbereitschaften bezüglich unterschiedlicher Produktgruppen haben kann.[38]

Schwierigkeiten für den Einsatz personalisierter Preise ergeben sich nicht zuletzt dadurch, dass die Kunden zunehmend Preissuchmaschinen nutzen. In diesem Kontext ist auch zu berücksichtigen, dass die Unternehmen im Wettbewerb mit anderen Anbietern stehen. Der Verbraucher versucht stets, den für ihn günstigsten Preis zu erzielen. Personalisierte Preise sind daher nur umsetzbar, wenn sie von einer Vielzahl der Unternehmen eingesetzt werden. Wobei auch dann das Risiko besteht, dass die einzelnen Anbieter zu unterschiedlichen Einschätzungen hinsichtlich der Preisbereitschaft eines Kunden kommen.[39] Einem einzelnen Anbieter kann der Einsatz personalisierter Preise nur gelingen, wenn seine Kunden immun gegen Preisvergleiche sind, das heißt, wenn eine große Bindung des Kunden an das Unternehmen besteht, wie es zum Beispiel bei vielen Amazon-Prime-Kunden der Fall ist.[40]

Für Unternehmen, die mehrere Vertriebskanäle nutzen, beispielsweise einen Online-Shop aber auch gleichzeitig Filialen betreiben, sowie für Franchise-Unternehmen ergeben sich zusätzliche Schwierigkeiten hinsichtlich der Umsetzung individueller Preise. Bei diesen Unternehmen herrscht die Ansicht vor, dass die Preise über alle Vertriebskanäle einheitlich sein sollen.[41] In Anbetracht der Tatsache, dass Kunden vielfach im Geschäft ihr Smartphone nutzen, um sich weitergehend über ein Produkt zu informieren oder gar um Preise zu vergleichen, erscheint der Anspruch einheitlicher Preise in diesem Kontext sinnvoll.[42] Zudem nehmen die Kunden den Anbieter, ungeachtet verschiedener Kanäle, derer er sich bedient, als einheitlichen Anbieter war.[43]

---

37 Schleusener, S. 79.

38 Schleusener, S. 77.

39 Schleusener, S. 77.

40 Schleusener, S. 81.

41 Schleusener, S. 77; Schleusener/Hosell, S. 12; Reinartz et al., S. 8.

42 Schleusener, S. 77.

43 Schleusener, S. 79.

b) Ablehnung durch die Verbraucher

Die Verbraucher nehmen personalisierte Preise grundsätzlich negativ wahr.[44] Studien zeigen, dass Konsumenten Preisunterschiede, unabhängig davon ob es sich um dynamische oder personalisierte Preise handelt, als unfair empfinden.[45] Dies betrifft sowohl diejenigen, die durch die Preisdifferenzierung einen Vorteil erlangt haben, als auch diejenigen, die benachteiligt wurden.[46] Zudem führt das Erleben von Preisdifferenzierungen dazu, dass die Wiederkaufsbereitschaft bei diesem Händler deutlich sinkt und das Vertrauen Schaden nimmt.[47] Nicht ohne Grund sind daher Unternehmen, die personalisierte Preise verwenden, um ein „Fencing" bemüht. Das sog. Fencing beschreibt die Bemühungen, differenzierte Preise dem Kunden nicht erkennbar werden zu lassen.[48]

Unterschiedliche Preise werden von den Konsumenten unter anderem dann akzeptiert, wenn die Kriterien für die Preisgestaltung erkennbar sind und branchenüblichen Normen entsprechen.[49] So ist bei Reisebuchungen bekannt, dass die besten Preise beim frühzeitigen Buchen erzielt werden können, da sich der Kunde dann schon früh festlegt. Jedoch kann auch bei Last-Minute-Angeboten ein günstiger Preis erzielt werden, belohnt wird hier die Flexibilität des Kunden. An dieser Stelle zeigt sich ein Kernproblem beim Einsatz personalisierter Preise. Für den Verbraucher ist weder nachvollziehbar, ob es sich überhaupt um einen personalisierten Preis handelt, noch nach welchen Kriterien dieser Preis zustande gekommen ist. Die Preisgestaltung erfolgt aus Sicht des Verbrauchers willkürlich.[50] Aufgrund dieser Intransparenz und der empfundenen Willkür werden individuelle Preise von der Mehrheit der Verbraucher als unfair

---

44 Obergfell, ZLR 2017, S. 290, 294; Reinartz et al., S. 13/16; Krämer/Kalka/Ziehe, S. 28, 35; Schleusener, S. 85; Verbraucherzentrale Bundesverband e.V., Personalisierte Preise, S. 4.

45 Reinartz/Haucap, S. 41; Reinartz et al., S. 13; Thorun/Diels, S. 8.

46 Reinartz/Haucap, S. 41.

47 Reinartz/Haucap, S. 42, 43; Reinartz et al., S. 14; Miller, Journal of Technology Law and Policy, S. 41, 85.

48 Reinartz et al., S. 9.

49 Reinartz et al., S. 11; Thorun/Diels, S. 9; Schleusener/Hosell, S. 14.

50 Reinartz et al., S. 14.

bewertet.[51] Als fair werden zum Beispiel Senioren- oder Studentenrabatte wahrgenommen, da diese Bevölkerungsgruppen üblicherweise ein geringeres Einkommen haben.[52] Werden hinter der Preisregel jedoch niedere Motive, wie zum Beispiel die schlichte Profitgier vermutet, lehnen die Konsumenten diesen Preis ab.[53] Gut akzeptiert werden auch Preisdifferenzierungen, auf deren Anwendung der Kunde Einfluss hat.[54] Hierzu gehören beispielsweise Rabatte aufgrund der Teilnahme an einem Loyalitätsprogramm.

Eine mögliche Reaktion der Verbraucher auf den Einsatz personalisierter Preise ist der Einsatz neuer Intermediäre.[55] Dabei könnte es sich um Anbieter handeln, die für den Kunden einen bestmöglichen Preis erzielen. Ebenso ist zu erwarten, dass Soft- und Hardwarelösungen entwickelt werden, die ähnlich wie die bereits bestehenden Adblocker dafür sorgen, dass preisrelevante Daten nicht weitergegeben werden.[56]

4. Aktuelle Verwendung

Der Einsatz personalisierter Preise kommt sowohl für den Offline- als auch für den Online-Handel in Betracht. Jedoch setzen in Deutschland derzeit, entgegen der öffentlichen Wahrnehmung, wohl nur wenige Unternehmen personalisierte Preise ein.[57] Anders sieht es bei der Verwendung von personalisierten Rabatten, insbesondere gestützt auf Kundenprogramme, aus.[58] Die geringe Nutzung von personalisierten Preisen wird insbesondere mit dem deutlich ablehnenden Verhalten der Kunden

---

51 Thorun/Diels, S. 8 f.; Reinartz et al., S. 14; Miller, S. 86.

52 Reinartz et al., S. 11; Zander-Hayat/Reisch/Steffen, VuR 2016, S. 403, 406.

53 Reinartz et al., S. 11.

54 Reinartz et al., S. 12; Miller, Journal of Technology Law and Policy, S. 41, 86.

55 Reinartz et al., S. 18; Schleusener/Hosell, S. 15.

56 Schleusener, S. 86; Schleusener/Hosell, S. 14; Reinartz et al., S. 18.

57 Zander-Hayat/Reisch/Steffen, VuR 2016, S. 403, 405; Reisch et al., S. 21; Schwaiger/Hufnagel, S. 43; Reinartz et al., S. 7; Krämer/Bornkamm/Feddersen, S. 35; Schleusener/Hosell, S. 22; Remmel, Wirtschaftsdienst 2016, S. 875, 876; Schleusener, S. 77; siehe auch A. III. 3.

58 Wenglorz, S. 961; Fezer/Büscher/Obergfell/Wenglorz, Rn. 81k.

begründet.[59] Zudem wird es als schwierig empfunden, mehrere Vertriebskanäle entsprechend zu harmonisieren und die Verwendung von Preissuchmaschinen zu unterbinden.[60]

Gerade im Online-Handel ist der Nachweis personalisierter Preise schwierig, da der einzelne Verbraucher keine Preisvergleiche anstellen kann. Aufgedeckt werden können solche Preise nur durch den zeitnahen Vergleich mit Preisen, die anderen Kunden angeboten werden. In Deutschland konnte bisher lediglich in der Tourismusbranche eine derartige Preisdifferenzierung festgestellt werden. So konnte in einer Studie eine Preisdifferenzierung nach bisherigem Surf- und Kaufverhalten sowie nach Betriebssystemen nachgewiesen werden.[61] In anderen Branchen konnte jedoch kein Einsatz personalisierter Preise festgestellt werden.[62]

Im stationären Handel werden in Deutschland bisher wohl kaum personalisierte Preise eingesetzt.[63] Im Gegensatz zum Online-Handel ist der Zugriff auf Kundendaten hier grundsätzlich begrenzt. Eine Möglichkeit, den Kunden zur freiwilligen Preisgabe seiner Daten zu bewegen, sind Kundenprogramme.[64] Möglich ist es auch, über Kameras, in der Zukunft sogar mit entsprechender Gesichtserkennungssoftware, Bluetooth oder WLAN-Netzwerke, die Bewegungen des Kunden zu beobachten.[65] Ein prominentes Beispiel für einen stationären Handel, der die Möglichkeit zur Anwendung von personalisierten Preisen hat, ist der Amazon-Go-Einzelhandel in Seattle.[66] Inwieweit die Preise personalisiert werden, ist jedoch nicht bekannt. Es gibt aber Supermärkte, die eine indirekte perso-

---

59 Schwaiger/Hufnagel, S. 45.

60 Schwaiger/Hufnagel, S. 46.

61 Schleusener/Hosell, S. 2/20.

62 Schleusener/Hosell, S. 2.

63 Zander-Hayat/Reisch/Steffen, VuR 2016, S. 403, 405.

64 Schwaiger/Hufnagel, S. 42.

65 Schwaiger/Hufnagel, S. 13; Miller, Journal of Technology Law and Policy, S. 41, 45.

66 https://www.zeit.de/wirtschaft/unternehmen/2016-12/amazon-go-supermarkt-lebensmittel-service-einkaufen-datenschutz-zukunft/komplettansicht (zuletzt abgerufen: 11/2018).

nalisierte Preisegestaltung durch Kundenkarten und personalisierte Rabatte erproben.[67] Anhand der Einkaufshistorie werden auf den Kunden zugeschnittene Rabatte generiert.[68]

IV. Rechtliche Aspekte

Neben technischen Herausforderungen und Akzeptanzproblemen bei den Verbrauchern, bestehen auch rechtliche Fragestellungen bei dem Einsatz personalisierter Preise.

1. Datenschutzrecht

Bei der Erstellung personalisierter Preise werden Kundendaten gesammelt, ausgewertet und zusammengeführt. Insbesondere der Einsatz von Big-Data-Anwendungen ermöglicht die Verarbeitung großer Datenmengen innerhalb kurzer Zeit. Dabei ist für die Verbraucher nicht mehr nachvollziehbar, was mit ihren Informationen geschieht, die sie beim Surfen im Internet hinterlassen. Häufig wissen selbst die Unternehmen nicht, was mit den Daten geschieht, die bei dem Besuch ihrer Webseite gesammelt werden.[69] Vor allem bei der Verwendung von Social-Media-Plug-Ins ist die weitere Nutzung der Daten nur schwierig nachzuvollziehen.[70] Diesem Informationsungleichgewicht soll durch das Datenschutzrecht begegnet werden. Aufgabe des Datenschutzrechts ist die Gewährleistung des Grundrechts auf informationelle Selbstbestimmung.[71] Dieses Grundrecht bestimmt, dass jeder das Recht hat, selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu bestimmen.[72]

Das Datenschutzrecht findet nur dann Anwendung, wenn es sich bei den fraglichen Informationen um Daten mit Personenbezug handelt (Art. 2

---

67 Zander-Hayat/Reisch/Steffen, VuR 2016, S. 403, 405.

68 Zander-Hayat/Reisch/Steffen, S. 403, 405; Obergfell, ZLR 2017, S. 290, 291 ff.; Wenglorz, S. 961.

69 Zander-Hayat/Reisch/Steffen, VuR 2016, S. 403, 408.

70 Zander-Hayat/Domurath/Groß, S. 5; Röttgen, S. 76 f.

71 Wolff/Brink/Wagner, Landesdatenschutz Rn. 25.

72 BVerfGE 65, 1 (43).

Abs. 1 Datenschutz-Grundverordnung [DS-GVO]). Die Bestimmung, unter welchen Umständen ein personenbezogenes Datum vorliegt, stellt eine der Hauptfragen des Datenschutzrechts dar.

a) Anonyme Daten

Anonyme Daten sind solche, bei denen keinerlei Personenbezug aufweisbar ist und ein solcher auch nicht mehr hergestellt werden kann.[73] Allerdings ist es schwierig festzustellen, wann ein Personenbezug vorliegt und wann es sich tatsächlich um anonyme Daten handelt. Es ist im Detail umstritten, wie das Merkmal des Personenbezugs zu definieren ist.[74] Lange Zeit war beispielsweise unklar, ob die IP-Adresse ein personenbezogenes Datum darstellt. Dies hat der BGH mittlerweile bestätigt.[75] Dazu kommt, dass die Zusammenführung verschiedener – für sich betrachtet anonymer Daten – letztlich zu einem Personenbezug führen kann.[76] Wenn viele Informationen wie z. B. Standort, verwendeter Browser, Betriebssystem, zusammengeführt werden, kann dies im Ergebnis einen Personenbezug ergeben.[77] Im BDSG (§ 3 Abs. 4 Nr. 6 BDSG aF) wurde eine Anonymisierung auch dann angenommen, wenn eine Zuordnung nur unter unverhältnismäßig hohem Aufwand möglich war. Die DS-GVO hingegen definiert den Begriff „Anonymisierung“ nicht. Generell ist wohl davon auszugehen, dass vor dem Hintergrund technischer Möglichkeiten bei der Verarbeitung von Daten nur noch selten ein „unverhältnismäßig hoher Aufwand“ angenommen werden kann.[78]

---

73 Schantz/Wolff, Rn. 297.

74 Härting, NJW 2013, S. 2065, 2066.

75 BGH, 16.05.2017 – VI ZR 135/13 = NJW 2017, S. 2416, 2417.

76 Schantz/Wolff, Rn. 300.

77 Schmidt, S. 1011.

78 Paal/Pauly/Ernst, Art. 4, Rn. 50 f.

Sofern für die Erstellung personalisierter Preise nur anonyme Daten verwendet werden, müssen die Vorschriften des Datenschutzrechts nicht beachtet werden.[79] Letztlich ist die Verarbeitung anonymer Daten für ein Unternehmen jedoch von geringer Relevanz, da viele, für die Preisbildung interessante Informationen, unberücksichtigt bleiben müssen.[80]

b) Pseudonyme Daten

Relevanter für Unternehmen ist die Verarbeitung pseudonymer Daten. Dies sind gem. Art. 4 Nr. 5 DS-GVO solche, die einer Person nicht ohne Hinzuziehung weiterer Informationen zugeordnet werden können. Diese zusätzlichen Informationen sind gesondert aufzubewahren.[81] Zu diesen pseudonymen Daten gehören zum Beispiel Cookies, bei denen nach wie vor umstritten ist, wie sie rechtskonform eingesetzt werden können.[82] Pseudonyme Daten werden wie personenbezogene Daten behandelt.[83]

Für eine pseudonyme Profilbildung hat § 15 Abs. 3 Telemediengesetz Anforderungen aufgestellt. Dieser findet seit der Geltung der DS-GVO wohl keine Anwendung mehr.[84] Eine solche auf Trackingdaten basierende Profilbildung könnte nun nach Art. 6 Abs. 1 lit. f DS-GVO zulässig sein. Danach ist eine Datenverarbeitung rechtmäßig, wenn sie zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte der betroffenen Personen überwiegen. Dabei könnte berücksichtigt werden, dass durch die Pseudonymität eine datenschutzfreundlichere Ausgestaltung

---

79 Erwägungsgrund 26, Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016.

80 Schmidt, S. 1011.

81 Schantz/Wolff, Rn. 304.

82 Rauer/Ettig, ZD 2018, S. 255, 256; Schmidt, S. 1011.

83 Erwägungsgrund 26, Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016.

84 Datenschutzkonferenz, Positionsbestimmung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder – Düsseldorf, 26. April 2018, https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Technik/Inhalt/TechnikundOrganisation/Inhalt/Zur-Anwendbarkeit-des-TMG-fuer-nicht-oeffentliche-Stellen-ab-dem-25_-Mai-2018/Positionsbestimmung-TMG.pdf (zuletzt abgerufen: 11/2018).

vorgenommen wird.[85] Im Hinblick auf Art. 5 Abs. 3 der ePrivacy-Richtlinie könnte aber beim Einsatz von Tracking-Mechanismen stets eine informierte Einwilligung nach Art. 6 Abs. 1 lit. a DS-GVO erforderlich sein.[86] Dies bleibt jedoch umstritten.[87] Eine Klärung könnte die geplante ePrivacy-Verordnung bringen.[88]

Sofern man davon ausgeht, dass eine Datenverarbeitung auch ohne ausdrückliche Einwilligung möglich ist, unterliegen die Unternehmen nach den Vorschriften der DS-GVO jedenfalls umfassenden Informationspflichten.[89] Dazu gehört insbesondere auch die Unterrichtung über den Zweck der Datenverarbeitung, also in diesem Fall die individuelle Preisgestaltung. Die Unterrichtung über die Datenverarbeitung kann beispielsweise in der Datenschutzerklärung der Webseite erfolgen.[90] Wird der Hinweis in der Datenschutzerklärung unterlassen, drohen dem Unternehmen empfindliche Bußgelder.

c) Personalisierte Datenverarbeitung

Eine personalisierte Datenverarbeitung liegt regelmäßig im Fall der individuellen Preise vor, wenn Daten wie z. B. die Bestellhistorie eines Kunden mit in die Datenverarbeitung, hier mit in die Preisbildung, einbezogen oder Trackingdaten mit einem Account verbunden werden.[91] Eine solche

---

85 Drewes, CR 2016, S. 721, 726.

86 Datenschutzkonferenz, Positionsbestimmung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder – Düsseldorf, 26. April 2018, https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Technik/Inhalt/TechnikundOrganisation/Inhalt/Zur-Anwendbarkeit-des-TMG-fuer-nicht-oeffentliche-Stellen-ab-dem-25_-Mai-2018/Positionsbestimmung-TMG.pdf (zuletzt abgerufen: 11/2018); Breyer, ZD 2018, S. 302, 303.

87 Gierschmann, ZD 2018, S. 297, 300; Stoklas, ZD-Aktuell 2018, 06123.

88 Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der RL 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation – ePrivacy-VO) vom 10.01.2017, COM(2017) 10 final.

89 Schmidt, S. 1012.

90 Schmidt, S. 1012.

91 Schmidt, S. 1013.

personalisierte Datenverarbeitung erfordert das Vorliegen eines Erlaubnistatbestandes des Art. 6 Abs. 1 DS-GVO. Nach Art. 6 Abs. 1 lit. b ist die Verarbeitung der personenbezogenen Daten zulässig, wenn sie zur Erfüllung eines Vertrags oder zur Durchführung einer vorvertraglichen Maßnahme erforderlich ist. Das wäre dann der Fall, wenn der Vertrag ohne die Datenverarbeitung nicht in dem Umfang erfüllt werden könnte, wie es mit der Datenverarbeitung der Fall wäre.[92] Zur Durchführung eines Vertrags können gerade im Online-Handel die Zahlungsinformationen sowie die Adresse des Kunden notwendig sein. Zwar könnte aus Sicht der Unternehmen eine Verarbeitung dieser Informationen für die Generierung personalisierter Preise sinnvoll erscheinen, erforderlich im Sinne des Art. 6 Abs. 1 lit. b DS-GVO ist sie aber für die Erfüllung des Vertrags jedenfalls nicht.[93]

Die Verarbeitung der personenbezogenen Daten könnte auch nach Art. 6 Abs. 1 lit. f DS-GVO rechtmäßig sein. Zwar könnte in der Datenverarbeitung zum Zwecke der Bildung personalisierter Preise ein berechtigtes Interesse wirtschaftlicher Art des Unternehmens vorliegen. Jedoch bestehen bereits Zweifel an der Erforderlichkeit.[94] Jedenfalls werden die Interessen und Grundrechte des Betroffenen die Interessen des Unternehmens überwiegen.[95]

Daher ist für die Nutzung personalisierter Preise eine ausdrückliche Einwilligung des Kunden (Art. 6 Abs. 1 lit. a DS-GVO) erforderlich.[96] In der Praxis kann eine solche Einwilligung über Vertragstexte bei der Anmeldung in einem Onlineshop oder beim Erwerb einer Kundenkarte erfolgen.[97] Die erteilte Einwilligung ist jedoch nur wirksam, wenn sie freiwillig und in Kenntnis der damit verbundenen Umstände und Konsequenzen erfolgt. Problematisch ist hier vor allem die erforderliche Transparenz der

---

92 Paal/Pauly/Frenzel, Art. 6, Rn. 14.

93 Zuiderveen Borgesius/Poort, S. 347, 360.

94 Zuiderveen Borgesius/Poort, S. 347, 360.

95 Zuiderveen Borgesius/Poort, S. 347, 360; Schmidt, S. 1013.

96 Hofmann, WRP 2016, S. 1074, 1075; Verbraucherzentrale Bundesverband e.V., Personalisierte Preise, S. 6.

97 Schmidt, S. 1013.

Belehrung, da die Kunden die hinter den personalisierten Preisen stehenden hochkomplexen Vorgänge kaum erfassen können.[98] Darüber hinaus muss bei der Einwilligung das Kopplungsverbot berücksichtigt werden. Danach darf eine vertragliche Leistung nicht von der datenschutzrechtlichen Einwilligung abhängig gemacht werden. Nach den Vorschriften der DS-GVO muss die Datenverarbeitung, die durch die Einwilligung gerechtfertigt werden soll, zumindest teilweise für die Leistungserbringung erforderlich sein (Art. 7 Abs. 4 DS-GVO).[99] Dies betrifft zum Beispiel Fälle, in denen die Nutzung einer Webseite von der Einwilligung in die Verwendung der Daten zum Zweck der Bildung personalisierter Preise abhängig gemacht wird.

d) Profiling

Nach Art. 22 Abs. 1 DS-GVO hat jede Person das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt. Art. 22 Abs. 1 DS-GVO erfasst auch das sog. Profiling. Dieses wird in Art. 4 Nr. 4 DS-GVO legal definiert als 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, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, persönlicher Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen.[100] Das Ergebnis eines Profilings kann die Bestimmung der Zahlungsbereitschaft, auf der personalisierte Preise beruhen, sein.[101] Jedoch muss die Entscheidung rechtliche Wirkung entfalten oder die Person in ähnlicher Weise erheblich beeinträchtigen. Durch die Anzeige eines Preises an sich wird keine rechtliche Wirkung entfaltet. Eine solche

---

98 Obergfell, ZLR 2017, S. 290, 295.

99 Schmidt, S. 1014; Tietjen/Flöter, GRUR-Prax 2017, S. 546, 547.

100 Siehe auch: Erwägungsgrund 71, Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016.

101 Paal/Pauly/Martini, Art. 22, Rn. 21.

wird erst angenommen, wenn der rechtliche Status des Betroffenen verändert wird.[102] Es muss eine erhebliche Beeinträchtigung des Betroffenen vorliegen, damit das Verbot des Art. 22 Abs. 1 DS-GVO greift. Eine solche liegt vor, wenn die Persönlichkeitsentfaltung nach objektiver Bewertung der Umstände des Einzelfalls durch eine Folge von einigem Gewicht beeinträchtigt wird.[103] Insbesondere können Beeinträchtigungen, die eine diskriminierende Wirkung haben, diese Schwelle erreichen.[104] Von personalisierten Preisen geht im Generellen keine solche erhebliche Beeinträchtigung aus. Im Einzelfall kann dies jedoch durchaus der Fall sein. Denkbar wäre dies zum Beispiel bei enormen Abweichungen vom Marktpreis, der geringen Verfügbarkeit der Ware oder dem Grad der Erforderlichkeit für den Betroffenen.[105]

2. Wettbewerbsrecht

Bei der Preisbildung gilt der Grundsatz der Preisgestaltungsfreiheit.[106] Die Höhe eines Preises, die Preisfairness und die zugrundeliegende Berechnung unterliegen keiner rechtlichen Kontrolle und letztere muss nicht offengelegt werden.[107] Dies erfasst auch den verwendeten Algorithmus.[108] Daher fordern einige Stimmen, dass zumindest die Kriterien, die der Preisbildung zugrunde gelegt werden, offen gelegt werden sollten.[109] Dies sei insbesondere deshalb unerlässlich, um etwaige Diskriminierungen zu erkennen und beanstanden zu können.[110] Eine entsprechende Pflicht besteht derzeit nicht und müsste gesetzlich geregelt werden.

Die durch den Unternehmer festgelegten Preise können zu jedem ihm sinnvoll erscheinenden Zeitpunkt nach Belieben erhöht oder gesenkt

---

102 Paal/Pauly/Martini, Art. 22, Rn. 26.

103 Paal/Pauly/Martini, Art. 22, Rn. 27; Schantz/Wolf, Rn. 737.

104 Paal/Pauly/Martini, Art. 22, Rn. 27.

105 Schantz/Wolf, Rn. 737.

106 Köhler/Bornkamm/Feddersen, § 5 Rn. 3.35; Tietjen/Flöter, GRUR-Prax 2017, S. 546, 547.

107 Hofmann, WRP 2016, S. 1074, 1077; Tietjen/Flöter, GRUR-Prax 2017, S. 546, 547; Genth, Wirtschaftsdienst 2016, S. 863, 864.

108 BGH, 28.1.2014 - VI ZR 156/13 = MMR 2014, S. 489, 491.

109 Zander-Hayat/Reisch/Steffen, VuR 2016 S. 403, 407.

110 Zander-Hayat/Reisch/Steffen, VuR 2016 S. 403, 407.

werden.[111] Jedoch müssen die Prinzipien der Preiswahrheit (§ 5 Abs. 1 S. 2 Nr. 2 Gesetz gegen den unlauteren Wettbewerb [UWG]) und Preisklarheit (§ 1 Abs. 6 S. 1 Preisangabenverordnung [PAngV]) berücksichtigt werden.

a) Irreführungsverbot

Ein Hindernis für personalisierte Preise kann das Irreführungsverbot des Wettbewerbsrechts (§ 5 UWG) darstellen. Danach handelt unlauter, wer eine irreführende geschäftliche Handlung vornimmt, die geeignet ist, den Verbraucher oder sonstigen Marktteilnehmer zu einer geschäftlichen Entscheidung zu veranlassen, die er andernfalls nicht getroffen hätte. Das Irreführungsverbot kennt in der Rechtswissenschaft eine Vielzahl von Anwendungsfällen. Beispielsweise darf der in einer Werbung angegebene Preis für ein Produkt in der Realität nicht zum Nachteil des Kunden abweichen.[112] Damit kann ein Händler die Preise nicht über den kundgegebenen Preis erhöhen. Dies gilt zumindest solange wie das Angebot läuft. Es besteht aber kein generelles Verbot der Preisdifferenzierung innerhalb desselben Geschäfts.[113] Nach wie vor kann ein Händler von einem Kunden heruntergehandelt werden und von anderen Kunden den ausgezeichneten Preis verlangen.

Im Online Handel können Irreführungen durch Preissuchmaschinen entstehen. Dies gilt sowohl für dynamische als auch für personalisierte Preise. Die von Händlern an die Preissuchmaschinen gemeldeten und dann durch letztere veröffentlichten Preise müssen einer höchstmöglichen Aktualität genügen.[114] Die Angabe eines veralteten Preises stellt eine irreführende geschäftliche Handlung dar.[115] Zudem dürfen Preise nicht systematisch, um „Mondpreise“ zu verschleiern oder willkürlich, herauf- und herabgesetzt werden.[116] Eine solche sog. Preisschaukelei wird angewendet, um die Kunden über die wahre Preislage zu täuschen und

---

111 BGH, 13.03.2003 – I ZR 212/00, S. 8 = NJW 2003, S. 2096, 2097.

112 BGH, 29.06.2000 – I ZR 29/98, S. 14 = NJW-RR 2001, S. 620, 622; Ullmann/Diekmann, § 5 Rn. 847; Tietjen/Flöter, GRUR-Prax 2017, S. 546, 547.

113 Köhler/Bornkamm/Feddersen, § 5 Rn. 3.37.

114 BGH, 11.03.2010 – I ZR 123/08, S. 7 = GRUR 2010, S. 936, 937.

115 Hofmann, WRP 2016, S. 1074, 1078; Köhler/Bornkamm/Feddersen, § 5 Rn. 3.40; Tietjen/Flöter, GRUR-Prax 2017, S. 546, 547.

116 BGH, 13.03.2003 – I ZR 212/00, S. 8 = NJW 2003, S. 2096, 2097.

so eine Unsicherheit zu erzeugen.[117] Bei personalisierten Preisen handelt es sich jedoch nicht um willkürliche Preisanpassungen, sondern um auf die Person des potentiellen Kunden zugeschnittene Preise. Dieser stellt die Summe der Gründe für den Preis dar. Demnach handelt es sich bei personalisierten Preisen aus dieser Sicht nicht um unlautere Geschäftspraktiken.

b) Aussagen des Preises

Ein individueller Preis könnte insofern als irreführend eingestuft werden, da verschwiegen bzw. nicht angezeigt wird, dass das nachgefragte Produkt im Durchschnitt günstiger angeboten wird.[118] Nach Nr. 19 des Anhangs zu § 3 Abs. 3 UWG stellt eine unwahre Angabe über die Marktbedingungen oder Bezugsquellen, um den Verbraucher dazu zu bewegen, eine Ware oder Dienstleistung zu weniger günstigen Bedingungen als den allgemeinen Marktbedingungen abzunehmen oder in Anspruch zu nehmen, eine unzulässige geschäftliche Handlung dar. Zu den Marktbedingungen gehören unter anderem die Umstände, die Einfluss auf das allgemeine Preisniveau haben.[119] Der Preis an sich sagt allerdings nichts über dessen Verhältnis zum Durchschnittspreis aus.[120] Es wird keine objektive falsche Information gegeben und auch kein Irrtum über die Marktbedingungen erregt.[121] Der Kunde kann jederzeit nach konkurrierenden, günstigeren Angeboten suchen. Zudem liegt keine Irreführung im Sinne des § 5 Abs. 1 S. 2 Nr. 2 UWG über die anbieterinternen Bedingungen vor. Danach ist eine geschäftliche Handlung irreführend, wenn sie unwahre Angaben enthält oder sonstige zur Täuschung geeignete Angaben über den Anlass des Verkaufs, wie das Vorhandensein eines besonderen Preisvorteils, den Preis oder die Art und Weise, in der er berechnet wird, oder die Bedingungen, unter denen die Ware geliefert oder die Dienstleistung erbracht wird, enthält. Eine Irreführung liegt dann nahe, wenn der angezeigte Preis vom tatsächlichen abweicht.[122] Bei personalisierten

---

117 Hofmann, WRP 2016, S. 1074, 1078; BGH, 14.12.1973 – I ZR 36/72, S. 12 = NJW 1974, S. 461, 462.

118 Hofmann, WRP 2016, S. 1074, 1080.

119 Obergfell, ZLR 2017, S. 290, 297.

120 Hofmann, WRP 2016, S. 1074, 1080; Obergfell, ZLR 2017, S. 290, 297; Tietjen/Flöter, GRUR-Prax 2017, S. 546, 548.

121 Obergfell, ZLR 2017, S. 290, 297.

122 Obergfell, ZLR 2017, S. 290, 297.

Preisen wird dem Nachfrager jedoch kein Preisvorteil vorgespielt. Ohne dass er dies erkennt, muss er im Vergleich zu einem anderen Kunden einen geringeren oder höheren Preis zahlen. Der angegebene Preis enthält nicht die Information, dass der Verkäufer das Produkt anderen Kunden nicht günstiger oder teurer anbietet.[123]

c) Preisangabenverordnung

Durch die PAngV soll die Position des Verbrauchers durch Schaffung eines optimalen Preisvergleichs gestärkt und der Wettbewerb gefördert werden.[124] Eine sachlich zutreffende und vollständige Verbraucherinformation gewährleistet nach Ansicht des Gesetzgebers Preisklarheit, Preistransparenz und Preiswahrheit.[125] Der Verbraucher muss in der Lage sein, sich erschöpfend durch Preisvergleiche über den Preisstand zu unterrichten.[126] Dies erfordert, dass die Preise untereinander vergleichbar sind.[127] Letztlich ermöglicht dies dem Verbraucher, sich für das günstigste Kauf- oder Leistungsangebot zu entscheiden und so den Wettbewerb zu fördern und einen Beitrag zur Dämpfung des Preisauftriebs zu leisten.[128] Die Bestimmungen der PAngV weisen Wettbewerbsbezug auf und stellen Marktverhaltensregelungen dar, sodass ein Verstoß über das Lauterkeitsrecht geahndet werden kann.[129] Im Zusammenhang mit personalisierten Preisen ist nun entscheidend, dass die PAngV nur Bestimmungen zur Angabe von Preisen enthält und nicht solche zur Preisbildung.[130] Entscheidender Gehalt der PAngV ist nur, dass die Preise vollständig, wahr und ohne weiteres erkennbar sein müssen.[131] Die PAngV erlaubt zudem die Gewährung von individuellen Preisnachlässen (§ 9

---

123 Hofmann, WRP 2016, S. 1074, 1080; Köhler/Bornkamm/Feddersen/, § 5, Rn. 3.38; Obergfell, ZLR 2017, S. 290, 297.

124 Ohly/Sosnitza, PAngV Einführung Rn. 17.

125 Ohly/Sosnitza, PAngV Einführung Rn. 17; Wenglorz, S. 962.

126 Ohly/Sosnitza, PAngV Einführung Rn. 1/17.

127 BGH, 21.05.1992 – I ZR 141/90 "Kilopreise IV" = GRUR 1992, S. 856, 857; Wenglorz, S. 962.

128 Ohly/Sosnitza, PAngV Einführung Rn. 17; BVerfGE 65, 248-265 (260) = GRUR 1984, S. 276, 279.

129 BGHZ 155, S. 301, 305; Wenglorz, S. 962.

130 Wenglorz, S. 962; Ohly/Sosnitza, PAngV Einführung Rn. 1.

131 Ohly/Sosnitza, PAngV § 1 Rn. 47.

Abs. 2 PAngV).[132] Es gibt keine Vorschriften dazu, dass ein Produkt allen Kunden zu demselben Preis verkauft werden muss oder der Preis über einen bestimmten Zeitraum stabil zu sein hat.[133] Personalisierte Preise sorgen daher nun dafür, dass die PAngV ihr Ziel, die Preistransparenz zu fördern, bei dieser Pricing-Strategie kaum noch erreichen kann.[134] Preisvergleiche werden immens behindert. Zu einer wahren und klaren Preisangabe gehört wohl auch, dass der Preis ein dynamischer oder personalisierter ist.[135]

d) Irreführung durch Unterlassen

Derzeit wird diskutiert, ob in Bezug auf die Verwendung personalisierter Preise eine Irreführung durch Unterlassen vorliegen könnte. Nach § 5a Abs. 2 UWG handelt insbesondere unlauter, wer einem Verbraucher eine wesentliche Information vorenthält, die der Verbraucher je nach den Umständen benötigt, um eine informierte geschäftliche Entscheidung zu treffen, und deren Vorenthalten geeignet ist, den Verbraucher zu einer geschäftlichen Entscheidung zu veranlassen, die er andernfalls nicht getroffen hätte. Zur Beurteilung, ob ein unlauteres Verhalten vorliegt, muss eine Abwägung der Interessen vorgenommen werden. Die Verwendung von personalisierten Preisen an sich könnte eine wesentliche Information darstellen. Dem kann man entgegnen, dass auch ohne diesen Hinweis ein Kunde in der Lage ist, eine informierte geschäftliche Entscheidung zu treffen. Das Risiko, irgendwo anders einen geringeren Preis zu zahlen, bestand schon immer. Derjenige, der Preise vergleicht und beispielsweise über Preissuchmaschinen nach dem günstigsten Angebot sucht, wird immer im Vorteil sein. Zudem rechnen Verbraucher verstärkt mit dem Gebrauch von personalisierten Pricing-Strategien, sodass der Hinweis auf solche kaum einen Mehrwert hätte. So gering dieser Mehrwert aber auch ist, so besteht jedoch ein berechtigtes Interesse der Verbraucher auf eine entsprechende Angabe. Zudem müssen auch solche Ver-

---

132 Wenglorz, S. 963.

133 Wenglorz, S. 964.

134 Wenglorz, S. 964/965.

135 Wenglorz, S. 965; Obergfell, ZLR 2017, S. 290, 299.

braucher geschützt werden, die nicht mit personalisierten Preisen rechnen oder diese nicht wahrnehmen.[136] Für eine informierte Entscheidung ist die Angabe, dass personalisierte Preise verwendet werden, wohl erforderlich.[137] Einige Stimmen leiten eine Hinweispflicht für personalisierte Rabatte im Online-Handel aus § 5a Abs. 4 i.V.m. § 6 Abs. 1 Nr. 3 TMG ab.[138] Diese Norm soll allerdings lediglich dafür sorgen, dass Kunden transparent und eindeutig über die Modalitäten von Rabatten informiert werden.[139] Eine Irreführung könnte aber dadurch gegeben sein, dass bei der Verwendung von personalisierten Preisen kein Durchschnitts- oder Referenzpreis angegeben wird. Eine solche Angabe forderte die Verbraucherzentrale NRW zur Landtagswahl in Nordrhein-Westfalen 2017.[140] Bei einem Referenzpreis handelt es sich um einen Vergleichspreis.[141] Diesen Preis ziehen Kunden bei der Beurteilung anderer Preise als Vergleichsmaßstab heran. Diese Angabe erscheint jedoch praktisch nicht umsetzbar, da die Referenzpreisforschung im höchsten Grade kompliziert und für die Händler nicht umsetzbar ist.[142] Die Händler sind aber in der Lage, den durchschnittlich von ihnen geforderten Preis anzugeben. Manche fordern sogar den Preisverlauf der letzten 72 Stunden mit dem jeweiligen Angebot offenzulegen.[143] Dabei spielt auch eine Rolle, dass durch den flächendeckenden Einsatz von personalisierten Preisen, die Verbraucher in Zukunft vielleicht nur noch schwierig Preise vergleichen können.[144] Derzeit ist dies noch der Fall, wobei bereits jetzt das Gefühl für den Wert

---

136 Zander-Hayat/Reisch/Steffen, VuR 2016, S. 403, 407; Reisch et al., S. 19; Schleusener, S. 83.

137 Obergfell, ZLR 2017, S. 290, 298; Zander-Hayat/Reisch/Steffen, VuR 2016, S. 403, 407/408.

138 Hofmann, WRP 2016, S. 1074, 1080.

139 Gersdorf/Paal/Pries, § 6 TMG, Rn. 8; Spindler/Schuster/Micklitz/Schirmbacher, § 6 TMG, Rn. 68-70.

140 Verbraucherzentrale Nordrhein-Westfalen e.V., Verbraucherproblemen wirksam begegnen – Weichen richtig stellen, S. 4.

141 Schwaiger/Hufnagel, S. 14.

142 Genth, Wirtschaftsdienst 2016, S. 863, 867.

143 Remmel, Wirtschaftsdienst 2016, S. 875, 877.

144 Zander-Hayat/Reisch/Steffen, VuR 2016, S. 403, 408; Kenning/Pohst, Wirtschaftsdienst 2016, S. 871, 874.

eines Produktes, zum Beispiel durch häufige Preisschwankung (dynamische Preise), beeinträchtigt ist.[145] Die Verbraucher haben durchaus ein berechtigtes Interesse daran, zu erfahren, wie sehr der von ihnen geforderte Preis von diesem Durchschnittspreis abweicht.[146] Dies gilt umso mehr, wenn vom Verbraucher abgeschöpfte Informationen zur Generierung des Preises herangezogen werden.[147] Zudem erfolgt die Personalisierung des Preises mit Hilfe von komplexen Algorithmen, die vom Verbraucher nicht nachvollzogen werden können.[148] Bei der Abwägung ist aber zu berücksichtigen, dass personalisierte Preise als Preisstrategie nicht unlauter sind und dem Händler letztlich auch eine Preisgestaltungs- und Vertragsfreiheit zukommt. Dies alles würde durch die Angabe eines Durchschnittspreises konterkariert. Kein Kunde würde einem Preis oberhalb dieses Durchschnittspreises zustimmen.[149]

e) Aggressive geschäftliche Handlungen

Das UWG untersagt in § 4a Abs. 1 S. 2 Nr. 3 und S. 3 UWG zudem aggressive geschäftliche Handlungen. Eine geschäftliche Handlung ist aggressiv, wenn sie geeignet ist, die Entscheidungsfreiheit des Verbrauchers unzulässig zu beeinflussen. Eine unzulässige Beeinflussung liegt vor, wenn der Unternehmer eine Machtposition gegenüber dem Verbraucher zur Ausübung von Druck in einer Weise ausnutzt, die die Fähigkeit des Verbrauchers zu einer informierten Entscheidung wesentlich einschränkt. Bei Unternehmen, die personalisierte Preise verwenden, kann man eine entsprechende Machtposition durchaus annehmen, da diese detaillierte Informationen über die Präferenzen jedes einzelnen Kunden haben. Die Kenntnisse der Unternehmen, gefördert unter anderem durch Big-Data-Anwendungen, sind weitreichend und übersteigen den Wissensstand des Kunden über sich selbst. Dies begründet eine strukturelle Überlegenheit[150], die über das generelle Ungleichgewicht zwischen Verbrauchern

---

145 Genth, Wirtschaftsdienst 2016, S. 863, 866; Remmel, Wirtschaftsdienst 2016, S. 875/876/877.

146 Obergfell, ZLR 2017, S. 290, 299.

147 Hofmann, WRP 2016, S. 1074, 1080/1081; Obergfell, ZLR 2017, S. 290, 299.

148 Obergfell, ZLR 2017, S. 290, 299; Zander-Hayat/Reisch/Steffen, VuR 2016, S. 403, 407.

149 Tietjen/Flöter, GRUR-Prax 2017, S. 546, 548.

150 Scherer, GRUR 2016, S. 233, 239.

und starken Unternehmen hinausgeht.[151] Die Unternehmen nutzten diese Machtposition jedoch nicht um Druck auszuüben.[152]

f) Unlauterkeit wegen des Allgemeinen Gleichbehandlungsgesetzes, § 3a UWG i.V.m. § 19 AGG

Personalisierte Preise sind grundsätzlich zulässig, da ein Angebot nicht die Aussage enthält, dass die Ware jedem Kunden zu dem gleichen Preis angeboten wird.[153] Zu berücksichtigen ist auch, dass es kein generelles Gleichbehandlungsgebot gibt, sodass die Preise nicht für alle gleich sein müssen.[154] Dennoch sind bestimmte Diskriminierungen als kritisch einzustufen. § 19 des Allgemeinen Gleichbehandlungsgesetzes (AGG) verbietet eine Benachteiligung aus Gründen der Rasse oder wegen der ethnischen Herkunft, wegen des Geschlechts, der Religion, einer Behinderung, des Alters oder der sexuellen Identität bei der Begründung, Durchführung und Beendigung zivilrechtlicher Massengeschäfte. Die Regelung des § 19 AGG stellt eine Marktverhaltensregel im Sinne des § 3a UWG dar, sodass ein Verstoß lauterkeitsrechtlich sanktionierbar ist.[155] Zwar enthält das AGG in § 20 eine Möglichkeit der Rechtfertigung von unterschiedlicher Behandlung, jedoch ist es zweifelhaft, ob allein die höhere Zahlungsbereitschaft eine unterschiedliche Preisgestaltung rechtfertigt.[156] Dies gilt insbesondere, wenn bestimmten Gruppen höhere Preise abverlangt werden als anderen. Zu berücksichtigen ist jedoch, dass bei personalisierten Preisen die in § 19 AGG genannten Kategorien zwar eine Rolle spielen können, es letztlich aber um die Abschöpfung einer möglichst großen Konsumentenrente jedes einzelnen Kunden geht. Es werden beispielweise Frauen nicht generell mit höheren Preisen konfrontiert als Männer. Somit kann beispielsweise einem Mann und einer Frau

---

151 Hofmann, WRP 2016, S. 1074, 1081; Fritzsche, WRP 2016, S. 1, 4.

152 Fritzsche, WRP 2016, S. 1, 4; Obergfell, ZLR 2017, S. 290, 300.

153 Hofmann, WRP 2016, S. 1074, 1078.

154 Köhler/Bornkamm/Feddersen, § 5 Rn. 3.36; Obergfell, ZLR 2017, S. 290, 300; Genth, Wirtschaftsdienst 2016, S. 863, 866; BGH, 18.04.1958 – I ZR 158/56 = GRUR 1958, S. 487, 489.

155 BT-Drucks. 16/1780, S. 48/49.

156 Hofmann, WRP 2016, S. 1074, 1079.

der gleiche, hohe Preis angezeigt werden, obwohl Frauen für das zugrundeliegende Produkt grundsätzlich eine höhere Zahlungsbereitschaft aufweisen würden.

g) Unlauterkeit wegen Verstoßes gegen das Datenschutzrecht

Ein Verstoß gegen das Datenschutzrecht ist nicht ohne weiteres wettbewerbswidrig.[157] Entscheidend ist, ob die verletzte Norm eine Marktverhaltensregel im Sinne des § 3a UWG darstellt. So kann sich der Marktbezug daraus ergeben, dass eine Vorschrift den Zweck verfolgt, den Betroffenen vor einer widerrechtlichen Nutzung seiner personenbezogenen Daten, zum Beispiel für Werbung, zu schützen.[158] Damit werden dem Marktverhalten Grenzen gesetzt, die den Schutz des Betroffenen in seiner Stellung als Marktteilnehmer bezwecken.[159] Ein Verstoß gegen das Datenschutzrecht kann daher unter Umständen auch unlauter nach dem UWG sein.

3. Kartellrecht

Aus kartellrechtlicher Sicht kommt eine Kontrolle der Preise zum einen in Betracht, wenn ein Unternehmen Marktmacht besitzt.[160] Eine marktbeherrschende Stellung ist per se nicht verwerflich, sondern erst dessen missbräuchliche Ausnutzung.[161] Im Hinblick auf personalisierte Preise ist festzuhalten, dass die Behinderung und Ungleichbehandlung von Marktteilnehmern integraler Bestandteil des Wettbewerbs ist.[162] Personalisierte Preise sind daher grundsätzlich auch nach dem Kartellrecht unbedenklich, solange nicht ein Unternehmen mit entsprechender Marktmacht diese missbräuchlich ausnutzt. Es bleibt jedoch zu berücksichtigen, dass ein marktbeherrschendes Unternehmen, welches personalisierte Preise verwendet, jeweils den Preis fordern wird, der der maximalen Zahlungsbereitschaft der Kunden entspricht.[163] Aufgrund fehlenden Wettbewerbs

---

157 Fezer/Büscher/Obergfell/Götting/Hetmank, UWG § 3a, Rn. 80.

158 Fezer/Büscher/Obergfell/Götting/Hetmank, UWG § 3a, Rn. 81.

159 Fezer/Büscher/Obergfell/Götting/Hetmank, UWG § 3a, Rn. 81.

160 Schulte/Just/Deister, § 19, Rn. 1.

161 Schulte/Just/Deister, § 19, Rn. 1.

162 Schulte/Just/Deister, § 19, Rn. 2/106.

163 Schleusener/Hosell, S. 7.

ist die Obergrenze für den zu fordernden Preis die maximale Preisbereitschaft des Kunden und nicht der Preis des Wettbewerbers.[164] Dies hat wohlfahrtsökonomische Nachteile, da eine Umverteilung des Gewinns von den Verbrauchern auf die Anbieter entsteht.[165]

Zum anderen kann dynamisches und personalisiertes Pricing zu einer Preisabsprache oder einem abgestimmten Verhalten führen (§ 1 Gesetz gegen Wettbewerbsbeschränkungen [GWB], Art. 101 Abs. 1 Vertrag über die Arbeitsweise der Europäischen Union [AEUV]), wenn zum Beispiel auf Preisalgorithmen und Datensätze ein und desselben Drittanbieters zurückgegriffen wird.[166] Dies kann dazu führen, dass alle Anbieter, die dieses System nutzen, dem einzelnen Kunden den gleichen Preis anbieten, sodass dieser kaum noch Auswahlmöglichkeiten hat. In diesem Fall würden die Preise steigen und die gesamte Preisbereitschaft der Kunden könnte abgeschöpft werden.[167] Dieses Szenario scheint auch einzutreten, wenn viele Unternehmen personalisierte Preise verwenden und sich deren verwendete Algorithmen immer stärker ähneln.[168] Dies dürfte sogar wahrscheinlich sein, da es immer nur einen „richtigen", der Preisbereitschaft entsprechenden, Preis geben kann.[169] Dieses rein faktische Angleichen der Preise würde vom Kartellrecht nicht erfasst werden. Abhilfe schaffen dann nur noch Wettbewerber, die versuchen, die hoch bepreisten Nachfrager als Kunden zu gewinnen. Zu berücksichtigen bleibt in jedem Fall, dass Algorithmen eine Preisabsprache deutlich vereinfachen und deren Nachweis deutlich erschweren.[170] Die Preisalgorithmen können sich gegenseitig beobachten und ohne Spuren aufeinander abgestimmt werden.[171]

---

164 Schleusener/Hosell, S. 7; Schleusener, S. 80.

165 Schleusener/Hosell, S. 6; siehe auch unter A. III. 2.

166 Ebers, NZKart 2016, S. 554; EuGH, 21.01.2016 – C-74/14 = EuZW 2016, S. 435-439; Monopolkommission, Rn. 167.

167 Schleusener, S. 80.

168 Schleusener, S. 82.

169 Schleusener, S. 82.

170 Kerler, Illegale Preisabsprachen: Drohen uns bald Algorithmus-Kartelle?, https://www.wired.de/article/preisabsprachen-durch-kuenstliche-intelligenz-drohen-uns-algorithmus-kartelle (zuletzt abgerufen: 11/2018); Monopolkommission, Rn. 171.

171 Monopolkommission, Rn. 185.

4. Allgemeines Zivilrecht

Personalisierte Preise sind nach dem allgemeinen Zivilrecht zulässig. Auch hier gilt das zum Lauterkeitsrecht Gesagte. Die Vertragsfreiheit gestattet es grundsätzlich Preise frei festzulegen.[172] Sie verstoßen weder gegen ein gesetzliches Verbot (§ 134 Bürgerliches Gesetzbuch [BGB]) noch gegen die guten Sitten (§ 138 BGB). Auch kann der Preis für eine Hauptleistungspflicht nicht im Wege der AGB-Inhaltskontrolle überprüft werden (§§ 305 ff. BGB).[173]

V. Fazit

Das Potential personalisierter Preise lässt sich derzeit noch nicht abschließend einschätzen. Insbesondere das ablehnende Konsumentenverhalten erscheint als ein erhebliches Hemmnis.[174] Als wesentlich für den Erfolg von personalisierten Preisen ist die Kommunikation der Preise anzusehen.[175] Zudem ist mit dem Entstehen von Intermediären, neben bereits existenten Preissuchmaschinen, zu rechnen, die beispielsweise das Kundenprofil verfälschen, um möglichst niedrige Preise zu erzielen.[176] Für bestimmte Bereiche ist die Anwendung von personalisierten Preisen besonders umstritten. Beispielsweise ist der Lebensmittelhandel, als ein zentraler Bestandteil der Grundversorgung, oder der Bereich von Versicherungen besonders problematisch.[177] Im Versicherungswesen besteht die Gefahr, dass personalisierte Preise das Solidaritätsprinzip der gesetzlichen Gesundheits- und Pflegeversicherung untergraben.[178]

Im Ergebnis sind personalisierte Preise aus rechtlicher Sicht grundsätzlich zulässig. Es gilt die Wettbewerbs- und Preisgestaltungsfreiheit, wel-

---

172 Obergfell, ZLR 2017, S. 290, 296.

173 Obergfell, ZLR 2017, S. 290, 296.

174 Schwaiger/Hufnagel, S. 20.

175 Schwaiger/Hufnagel, S. 20; http://www.absatzwirtschaft.de/birgt-dynamisches-und-personalisiertes-pricing-rechtliche-probleme-fuer-handel-und-dienstleister-100941/ (zuletzt abgerufen: 11/2018).

176 Schwaiger/Hufnagel, S. 21.

177 Obergfell, ZLR 2017, S. 290, 292.

178 Verbraucherzentrale Bundesverband e.V., Personalisierte Preise, S. 7.

che gerade auch umfassen, Kunden unterschiedlich behandeln zu dürfen.[179] Händler handeln nicht unlauter, wenn sie mit unterschiedlichen Preisen werben oder unterschiedliche Preise, gegebenenfalls auch unterschieden nach Ort oder Vertriebsweg, fordern.[180] Ein generelles Gleichbehandlungsgebot lässt sich mit einem freien Markt, in dem sich die Preise beeinflusst durch den Wettbewerb ergeben, nicht vereinbaren.[181] Zudem ist zu berücksichtigen, dass solange der Markt funktioniert, davon auszugehen ist, dass Alternativen entstehen werden. Beispielsweise können Händler damit werben, dass sie keine personalisierten Preise verwenden.

Es bleibt jedoch zu überlegen, ob gesetzlich eine Pflicht geschaffen werden sollte, dass direkt an dem jeweiligen Preis auf eine personalisierte Preisgestaltung hinzuweisen ist.[182] Dies würde den Verbraucherschutz erhöhen und den Verbraucher zu einem Preisvergleich animieren. Dabei ist auch zu berücksichtigen, dass der Verbraucher mehr unfreiwillig als freiwillig seine Daten für die Bildung von personalisierten Preisen zur Verfügung stellt und dann der Preisbildung ohne Möglichkeit der Einflussnahme unterworfen ist. Der Verbraucher liefert letztlich alle Informationen, um von ihm selbst einen möglichst hohen, der Zahlungsbereitschaft entsprechenden, Preis von ihm fordern zu können. Überträgt man dieses Machtgefüge auf einen klassischen Marktkauf, wäre es dort so, dass der Käufer dem Verkäufer, bevor dieser den Kaufpreis nennt, seinen Maximalpreis nennt.[183] Unter diesen Gesichtspunkten ist eine Kennzeichnungspflicht wohl mehr als angemessen. Viele Kunden wissen zwar grundsätzlich um die Existenz von personalisierten Preisen, aber sie sind sich der Personalisierung des Preises im konkreten Einkaufsvorgang nicht immer bewusst.[184] Zudem ist sicherzustellen, dass eine Verweigerung der Datenverarbeitung, welche der Personalisierung von Preisen dient, nicht zu einer Zugangsdiskriminierung führt.[185] Ansonsten könnten

---

179 Hofmann, WRP 2016, S. 1074, 1081; Köhler/Bornkamm/Feddersen, § 5, Rn. 3.36.

180 Köhler/Bornkamm/Feddersen, § 5, Rn. 3.36.

181 Köhler/Bornkamm/Feddersen, § 5, Rn. 3.36; Schulte/Just/Deister, § 19, Rn. 2.

182 Wenglorz, S. 965; Tietjen/Flöter, GRUR-Prax 2017, S. 546, 548.

183 Miller, Journal of Technology Law and Privacy, S. 41, 46.

184 Obergfell, ZLR 2017, S. 290, 294.

185 Verbraucherzentrale Bundesverband e.V., Personalisierte Preise, S. 7.

bestimmte Konsumentengruppen von wichtigen Versorgungsplattformen abgeschnitten sein.

Literaturnachweise

Breyer, Datenschutz im Internet: Zwangsidentifizierung und Surfprotokollierung bleiben verboten, ZD 2018, S. 302-303.

Dammann, Erfolge und Defizite der EU-Datenschutzgrundverordnung, Erwarteter Fortschritt, Schwächen und überraschende Innovationen, ZD 2016, S. 307-314.

Drewes, Dialogmarketing nach der DSGVO ohne Einwilligung der Betroffenen, CR 2016, S. 721-729.

Ebers, Dynamic Algorithmic Pricing: Abgestimmte Verhaltensweise oder rechtmäßiges Parallelverhalten?, NZKart 2016, S. 554-555.

Fezer/Büscher/Obergfell, UWG, 3. Auflage München 2016.

Fritzsche, Aggressive Geschäftspraktiken nach dem neuen § 4 a UWG, WRP 2016, S. 1-8.

Genth, Dynamische Preise: ein Gewinn für Handel und Verbraucher, Wirtschaftsdienst 2016, S. 863-868.

Gersdorf/Paal, Beck´scher Online-Kommentar Informations- und Medienrecht, 19. Edition 2018.

Gierschmann, Positionsbestimmung der DSK zur Anwendbarkeit des TMG, ZD 2018, S. 297-301.

Härting, Anonymität und Pseudonymität im Datenschutzrecht, NJW 2013, S. 2065-2071.

Hofmann, Der maßgeschneiderte Preis, Dynamische und individuelle Preise aus lauterkeitsrechtlicher Sicht, WRP 2016, S. 1074-1082.

Kenning/Pohst, Die verbraucherwissenschaftliche Perspektive: von der Customer Confusion zur Price Confusion, Wirtschaftsdienst 2016, S. 871-874.

Köhler/Bornkamm/Feddersen, Gesetz gegen den unlauteren Wettbewerb, 36. Auflage München 2018.

Krämer/Kalka/Ziehe, Personalisiertes und dynamisches Pricing aus Einzelhandels- und Verbrauchersicht, Marketing Review St. Gallen 6/2016, S. 28-37.

Miller, What do we worry about when we worry about price discrimination? The law and ethics of using personal information for pricing?, Journal of Technology Law and Policy 2014, S. 41-104.

Monopolkommission, Wettbewerb 2018 XXII. Hauptgutachten der Monopolkommission gemäß § 44 Abs. 1 S. 1 GWB, Baden-Baden 2018.

Obergfell, Personalisierte Preise im Lebensmittelhandel – Vertragsfreiheit oder Kundenbetrug?, ZLR 2017, S. 290-301.

Ohly/Sosnitza, Gesetz gegen den unlauteren Wettbewerb, 7. Auflage München 2016.

Paal/Pauly, Datenschutz-Grundverordnung/Bundesdatenschutzgesetz, 2. Auflage München 2018.

Rauer/Ettig, Rechtskonformer Einsatz von Cookies, ZD 2018, S. 255-258.

Reinartz/Haucap, Preisdifferenzierung im Handel, 2017.

Reinartz et al., Preisdifferenzierung und -dispersion im Handel, 2017.

Reisch et al., Digitale Welt und Handel. Verbraucher im personalisierten Online-Handel, Sachverständigenrat für Verbraucherfragen, Berlin 2016.

Remmel, Die verbraucherpolitische Perspektive: aktuelle Entwicklungen im Online-Handel, Wirtschaftsdienst 2016, S. 875-877.

Röttgen, Gefällt mir, gefällt mir nicht – Tracking im Internet, in: Hoeren/Kolany-Raiser (Hrsg.), Big Data zwischen Kausalität und Korrelation, S. 84-94, Münster 2016.

Schantz/Wolff, Das neue Datenschutzrecht, München 2017.

Scherer, Die Neuregelung der aggressiven geschäftlichen Handlungen in § 4 a UWG, GRUR 2016, S. 233-242.

Schleusener, Personalisierte Preise im Handel – Chancen und Herausforderungen, in: Stüber/Hudetz (Hrsg.), Praxis der Personalisierung im Handel, Wiesbaden 2017.

Schleusener/Hosell, Expertise zum Thema „Personalisierte Preisdifferenzierung im Online-Handel“, Berlin 2016.

Schmidt, Dynamische und personalisierte Preise – datenschutz-, wettbewerbs- und kartellrechtliche Grenzen, in: Tagungsband DSRI-Herbstakademie 2016, Smart World – Smart Law? Weltweite Netze mit regionaler Regulierung.

Schulte/Just, Kartellrecht, 2. Auflage Köln 2015.

Schwaiger/Hufnagel, ABIDA-Gutachten „Handel und elektronische Bezahlsysteme“, http://www.abida.de/sites/default/files/Gutachten_Handel_Bezahlsysteme.pdf (zuletzt abgerufen: 11/2018).

Spindler/Schuster, Recht der elektronischen Medien, 3. Auflage München 2015.

Stoklas, Die Anwendbarkeit des TMG für nicht-öffentliche Stellen ab 25.5.2018, ZD-Aktuell 2018, 06123.

Thorun/Diels, Was Verbraucherinnen und Verbraucher in NRW über individualisierte Preise im Online-Handel denken, Abschlussbericht, Berlin 2016.

Tietjen/Flöter, Dynamische und personalisierte Preise: Welche lauterkeitsrechtlichen Schranken gelten für Unternehmen?, GRUR-Prax 2017, S. 546-548.

Ullmann, UWG, 4. Auflage Saarbrücken 2016.

Verbraucherzentrale Bundesverband e.V., Personalisierte Preise, Diskussionspapier des Verbraucherzentrale Bundesverbands, 2016, https://www.vzbv.de/sites/default/files/vzbv_position_preisdifferenzierung_16-09-21_pdf.pdf.

Verbraucherzentrale Nordrhein-Westfalen e.V., Verbraucherproblemen wirksam begegnen – Weichen richtig stellen, Forderungen der Verbraucherzentrale NRW zur Landtagswahl Nordrhein-Westfalen, 2017, https://www.verbraucherzentrale.nrw/sites/default/files/migration_files/media247515A.pdf (zuletzt abgerufen: 11/2018).

Wenglorz, Dynamischer Preis: Ein Fall für die Preisangabenverordnung?, in: Büscher et al., Festschrift für Karl-Heinz Fezer zum 70. Geburtstag, Marktkommunikation zwischen Geistigem Eigentum und Verbraucherschutz, München 2016.

Wolff/Brink, Beck´scher Online-Kommentar Datenschutzrecht, 23. Edition 2018.

Zander-Hayat/Domurath/Groß, Personalisierte Preise, SVRV Working Paper Nr. 2, Berlin 2016.

Zander-Hayat/Reisch/Steffen, Personalisierte Preise – Eine verbraucherpolitische Einordnung, VuR 2016, S. 403-410.

Zuiderveen Borgesius/Poort, Online Price Discrimination and EU Data Privacy Law, J Consum Policy 2017, S. 347-366.

N. Daten-Doping: Big Data im Profisport (Christian Straker und Tristan Julian Tillmann[1])

Stand: Oktober 2018

Abstract: Daten-Doping: Big Data im Profisport

Der Einsatz technischer Hilfsmittel im Profisport nimmt immer stärker zu und verändert diesen grundlegend. Big-Data-Anwendungen erlauben die Überwachung der Leistung einzelner Athleten, die Analyse von Taktiken und sogar eine Prognose über das Entwicklungspotential junger Talente. Daher mag man sich nun fragen: Sind Daten eine neue Form des Dopings, ohne die man im Konkurrenzkampf des Profisports ins Hintertreffen gerät? Der vorliegende Beitrag zeigt auf, welche technischen Hilfsmittel bereits eingesetzt werden und zieht den Vergleich zu traditionellem Doping. Außerdem wird der Frage nachgegangen, ob die tragenden Gründe für das Verbot von Doping im Sport ebenso dafür sprechen, den Einsatz von Big-Data-Anwendungen im Sport einzuschränken oder gar zu untersagen.

I. „Daten-Doping“: Der Siegeszug der Daten im Profisport

Das Beispiel von „Moneyball“ ist bereits häufig bemüht worden. Eine Mannschaft von Underdogs, denen niemand einen großen Erfolg zugetraut hätte, entpuppt sich als kluge Zusammenstellung von Individualisten, die über „verborgene Talente“ verfügen, diese im Kollektiv abrufen und letztlich als Ganzes überraschen. Die kluge Zusammenstellung und das Entdecken der verborgenen Talente basierte hierbei auf datengestützten Erkenntnissen. Diese, so das Narrativ von Big Data im Profisport,

[1] Die Verfasser danken Alexander Weitz und Jan Tegethoff für die Unterstützung bei der Erstellung des Beitrags.

beruhen auf nachgewiesenen oder zumindest belegbaren Ursache-Wirkungs-Zusammenhängen. Freut man sich im Beispiel von Moneyball mit den Underdogs darüber, dass sie ihre Unterlegenheit überwinden können, so darf dies nicht darüber hinwegtäuschen, dass der Einsatz technischer Hilfsmittel im Profisport auch negative Auswirkungen haben kann. Hierbei ist der Vergleich zu leistungsfördernden Substanzen gar nicht so weit hergeholt. Big-Data-Anwendungen im Profisport haben ähnlich wie leistungsfördernde Substanzen das Potential, die Leistungen einzelner Athleten und sogar ganzer Mannschaften zu optimieren. Sowohl der Einsatz von Dopingmitteln als auch die Verwendung technischer Hilfsmittel im Sport sind zur gleichen Zeit aber auch Gegenstand von Kritik. Im Gegensatz zum Verbot von Doping wird die Ablehnung von technischen Hilfsmitteln im Sport nicht durch einen breiten gesellschaftlichen Konsens getragen.[2]

Insofern bietet eine Analyse dieses Konsenses einen guten Ausgangspunkt, um über die Rolle von Big-Data-Anwendungen als technische Hilfsmittel im Sport nachzudenken. Denn die Doping-Thematik bietet eine spezifische Perspektive auf die generelle Debatte über die künstliche Verbesserung des Menschen. Begriffe wie „Hirndoping“ und „Gendoping“ haben Einzug in den Diskurs gehalten. Wie weit kann und soll die künstliche Verbesserung des Menschen, das Human Enhancement, vorangetrieben werden? Der Sport und die Frage, inwieweit Doping erlaubt sein sollte, spiegelt diese gesellschaftliche Debatte wieder. Die Vorbildfunktion, die der Sport für die Gesellschaft allgemein einnimmt, wird durch ein Zitat von Albert Camus verdeutlicht:

„Denn auch wenn mir die Welt in all den Jahren einiges geboten hat, alles, was ich schließlich am sichersten über Moral und menschliche Verpflichtungen weiß, verdanke ich dem Sport“.[3]

Wirft man nun einen Blick auf den Einsatz der bereits heute zahlreichen Big-Data-Anwendungen im Profisport, dann lässt sich etwas plakativ

---

2 Vgl. NADA Austria, Warum ist Doping verboten?, https://www.nada.at/de/praevention/dopipedia/marketshow-warum-ist-doping-verboten (zuletzt aufgerufen am 20.09.2018).

3 Camus.

durchaus von „Daten-Doping“ sprechen. Wenn dem aber so ist, muss die Frage erlaubt sein, ob datenbasierte technische Hilfsmittel stärker reglementiert oder gar verboten werden sollten.

II. Dopingverbote im Leistungssport

Als umfassendes Regelwerk zum Doping im Sport ist der World Anti-Doping Code (WADC) der World Anti-Doping Agency (WADA) hervorzuheben. Basierend hierauf besteht als nationale Regelung in Deutschland der Nationale Anti-Doping Code (NADC) der Nationalen Anti-Doping Agentur (NADA). Art. 2 des NADC führt zehn Tatbestände auf, die Verstöße gegen die Anti-Doping-Bestimmungen normieren: Zentral sind hierbei nach Art. 2 Nr. 1 das Vorhandensein einer Verbotenen Substanz, ihrer Metaboliten oder Marker in der Probe eines Athleten sowie gem. Art. 2 Nr. 2 der Gebrauch oder der Versuch des Gebrauchs einer Verbotenen Substanz oder einer Verbotenen Methode durch einen Athleten als Verstoß gegen die Anti-Doping-Bestimmungen.[4] Daneben bestehen für die jeweilige Sportart spezifische Regelwerke.[5]

III. Begründungen für Dopingverbote im Profisport

Fraglich ist, aus welchen Erwägungen heraus sich der zuvor erwähnte breite Konsens für derartige Verbote begründet. Im Wesentlichen lassen sich drei Begründungsstränge unterscheiden: Chancengleichheit, medizinische Gründe und die Natürlichkeit des Sports.[6]

Die zum Doping verwendeten verbotenen Substanzen und Methoden dienen dem einzelnen Athleten zur Leistungssteigerung. Sind Dopingmittel für alle Athleten erlaubt, so besitzen formal alle auch die gleichen Chancen. Denn für alle gelten die gleichen Spielregeln. Die Substanzen und Methoden sind allerdings nicht für alle in gleichem Maße tatsächlich

---

4 Nationale Anti-Doping Agentur Deutschland, Nationaler Anti-Doping Code 2015, S. 10 ff.

5 Siehe für den Fußball zum Beispiel die Regeln des Weltfußballverbands FIFA, FIFA 2018.

6 FIFA 2018, S. 9.

verfügbar. Ursache hierfür kann zum Beispiel eine unterschiedliche finanzielle Ausstattung der Athleten sein. Wenn ein Athlet ein ganzes Team von Doping-Experten hinter sich weiß und ein anderer Athlet ein solches Team schlicht nicht finanzieren kann, lässt sich kaum von Chancengleichheit sprechen. Im Vordergrund steht dann nicht der sportliche Wettkampf, sondern die finanzielle Leistungsfähigkeit.

Das zentrale Argument gegen den Einsatz von leistungssteigernden Substanzen sind medizinische Bedenken. Tragender Grund für das Verbot des „klassischen" Dopings ist das mit der Einnahme leistungssteigernder Substanzen verbundene medizinische Risiko für die Athleten.[7] Deutlich zeigen sich die Folgen von Doping anhand der Sportler der ehemaligen DDR, welche heute unter zum Teil gravierenden Erkrankungen leiden und frühzeitig versterben.[8] Nicht ohne Grund sieht der EGMR die Rechtfertigung für weitgehende Eingriffe in die Privatsphäre der Sportler im Rahmen von Dopingkontrollen im Gesundheitsschutz.[9] In diesem Zusammenhang besteht auch eine mittelbare Komponente, die es nicht zu unterschätzen gilt. Der EGMR spricht explizit an, dass der Gesichtspunkt des Gesundheitsschutzes im Zusammenhang mit der Vorbildfunktion für Kinder und Jugendliche steht. Welche Eltern würden noch guten Gewissens ihre Kinder zum Sport schicken, wenn sie wüssten, dass diese möglicherweise früher oder später in Kontakt mit gefährlichen Medikamenten kommen könnten. Dies könnte zu einer beträchtlichen Schwächung des Breitensports und zu einer dramatischen Verschlechterung des Gesundheitszustandes der Bevölkerung führen. Ganz zu schweigen von den daraus resultierenden (Folge-)Kosten, die von der Gesellschaft über Krankenkassenbeiträge zu finanzieren wären.

Ein weiterer Begründungsansatz stellt auf die Natürlichkeit des Sports ab. Leistungssport soll eine Demonstration dessen sein, was der Mensch aus

---

7 NADA Austria, Warum ist Doping verboten?, https://www.nada.at/de/praevention/dopipedia/marketshow-warum-ist-doping-verboten (zuletzt aufgerufen am 20.09.2018).

8 Fritsch, Vergiftet von der DDR, https://www.zeit.de/sport/2018-02/doping-ddr-sport-dopingopfer-kinder-folgen-hilfe/komplettansicht (zuletzt aufgerufen am 04.10.2018).

9 EGMR, Urt. v. 18.01.2018, Az. 48151/11 u. 77769/13 = SpuRt 2018, 62-67, 65.

eigener Kraft zu leisten imstande ist.[10] Der Sport stellt eine Inszenierung dessen dar, wozu der Mensch kraft Übung und Talent zu leisten in der Lage ist.[11] Der Grundgedanke besteht darin, „eine Leistung mit eigenen Mitteln hervorzubringen, mit den Fähigkeiten des eigenen Körpers und dem Können, Willen und Wissen, die der Athlet in seinem Training einsetzt".[12] Werden künstliche Mittel zur Leistungssteigerung verwendet, wird diese Funktion des Sports in Frage gestellt. Durch den Einsatz künstlicher Maßnahmen zur Leistungssteigerung beruht die Leistung des Sportlers nicht mehr auf Talent, Disziplin und Trainingsfleiß.[13] Damit steht nicht mehr der Sportler als Athlet im Vordergrund, sondern das technische Entwicklerteam hinter ihm.

Die Sportfachverbände setzen mit ihren Bestimmungen bestimmte Grenzen fest, wann es sich um eine verbotene Substanz oder verbotene Methode handelt. Es ist klar, dass die Athleten, vor allem im stark kommerzialisierten Leistungssport, bemüht sind, die Grenzen auszureizen.

IV. Big-Data-Anwendungen im Profisport

Die Digitalisierung und nun auch Big-Data-Anwendungen bieten für nahezu jede Sportart ein enormes Potential zur Verbesserung der Leistung der Athleten. Einige Sportarten, wie zum Beispiel Baseball, sind auf Grund der Singularität der Abläufe bzw. deren Unterteilbarkeit besonders geeignet für eine datengetriebene Auswertung und Optimierung. Im Baseball fand dies schon relativ früh statt. Das liegt vor allem daran, dass bereits seit der Gründung der Major League Baseball (MLB), der Nord-

---

10 NADA Austria, Warum ist Doping verboten?, https://www.nada.at/de/praevention/dopipedia/marketshow-warum-ist-doping-verboten (zuletzt aufgerufen am 20.09.2018).

11 Pawlenka, S. 6.

12 Gebauer, Doping jetzt freigeben? Nein, nie!, https://www.zeit.de/sport/2013-02/doping-sport-freigabe-contra-missbrauch-gebauer-philosophisches-armdruecken/komplettansicht (zuletzt aufgerufen am 20.09.2018).

13 Wagner/Castronova, Doping freigeben? Ja, jetzt und kontrolliert!, https://www.zeit.de/sport/2013-02/doping-duell-freigabe-pro-missbrauch-wagner-philosophisches-armdruecken/komplettansicht (zuletzt aufgerufen am 20.09.2018).

amerikanischen Profiliga, Statikstiken mit enormer Akribie geführt werden.[14] Sie sind integraler Bestandteil der Baseball-Kultur.[15] Über jeden Spieler und jedes Team wird eine Vielzahl von Werten bereitgehalten, die mal mehr und mal weniger aussagekräftig sind. Nur beispielhaft genannt seien die ERA (Earned Run Average), die angibt, wie viele gegnerische Runs (Punkte) ein Pitcher (Werfer) durchschnittlich in neun Innings (Spiele) zulässt und die AVG (Batting Average), welche deutlich macht, wie hoch die Wahrscheinlichkeit ist, dass der Batter (Schlagmann) bei einem regulären Wurf mindestens die erste Base erreicht. Von diesen Daten aus war es nur ein relativ kleiner Schritt zu der Verwendung von computergestützten Statistikverfahren zur Zusammenstellung von Teams.

Andere Sportarten hingegen konnten lange Zeit nicht oder nicht richtig digital erfasst werden. Zu diesen Sportarten gehören die sogenannten Invasion Sports. Diese zeichnen sich dadurch aus, dass zwei Teams in einem festgelegten Feld um den Besitz eines Spielgerätes konkurrieren und versuchen, Punkte bzw. Tore zu erzielen, indem sie das Spielgerät in den gegnerischen Bereich transportieren, während sie gleichzeitig ihren eigenen Bereich verteidigen müssen.[16] Dazu gehören zum Beispiel Fußball, Basketball, Eishockey oder Handball. Doch auch bei diesen Sportarten wird mittlerweile verstärkt auf digitale Hilfe gesetzt. Die gewonnenen Daten halten bereits über „Heat-Maps“ und realtaktische Aufstellungen bei Fußballübertragungen Einzug in die heimischen Wohnzimmer. Im Ergebnis weisen die Invasion Sports jedoch eine Komplexität auf, die es schwer erscheinen lässt, konkrete Aussagen aus den an sich einfach zu sammelnden Daten abzuleiten. Den ersten noch recht einfachen Schritt haben Teams in der finnischen Eishockeyliga (Liiga) gemacht, indem sie den Herzschlag der Spieler überwachten und einem Spieler eine Auszeit gaben, sobald sich dessen Pulsschlag der maximalen Herzfrequenz näherte.[17] Dies ist jedoch noch weit entfernt von der Erstellung von

---

14 Sands et al., S. S2-64.

15 Lamoreaux, S. 598.

16 Gudmundsson/Horton, S. 22.1.

17 Fischer, Wie Datenanalyse den Leistungssport verändert, https://www.welt.de/gesundheit/article153950153/Wie-Datenanalyse-den-Leistungssport-veraendert.html (zuletzt aufgerufen am 21.09.2018).

Prognosen oder komplexeren Aussagen über Taktik und Teamperformance. Als ein zentraler Faktor für den Erfolg eines Teams gilt beispielsweise dessen Fähigkeit, das Spielfeld zu kontrollieren.[18] Doch wann ist dies der Fall bzw. in wie viele und welche Sektoren/Felder soll ein Spielfeld unterteilt werden, um entsprechend genaue Ergebnisse zu erreichen? Daran anknüpfend stellen sich Fragen zur Interaktion der Teammitglieder untereinander und ob es Schlüsselspieler gibt, deren Leistung oder Qualität auch die der Mitspieler steigert.[19] Im Bereich des Basketballs wurden sogar bereits sogenannte künstliche neuronale Netze, die einen Zweig der künstlichen Intelligenz darstellen, eingesetzt. Diese konnten Angriffsspiele automatisch und in Echtzeit erkennen und klassifizieren. Zudem ist es damit möglich, die Wahrscheinlichkeit zu bestimmen, mit der ein Korb erzielt wird.[20] Eine solche Erfassung der Taktik unterscheidet sich deutlich von den bereits seit längerem ermittelten Werten, wie der zurückgelegten Distanz eines Spielers oder dessen Geschwindigkeit.[21]

Letztendlich verfolgen die Digitalisierung und mit ihr alle neuen Big-Data-Anwendungen im Sport auch das Ziel, dem sportlichen Ereignis die Unberechenbarkeit zu nehmen. Trainer, Sportler und auch Sportwettende würden nur allzu gern bereits vorher wissen, wie der Wettkampf endet bzw. was sie tun müssen, damit sie gewinnen. Letzteres bezieht sich sowohl auf die Vorbereitung als auch auf mögliche Reaktionen während des Wettbewerbes selbst, wie zum Beispiel Einwechselungen oder Veränderungen an der Spielformation. Big Data soll die Taktik-Entscheidungen der Trainer validieren, individuellen Fortschritt der Athleten sicherstellen und neue Spieltaktiken von Kontrahenten erkennen und entschlüsseln.[22]

Darüber hinaus wird Big Data auch im Umfeld von Sportveranstaltungen genutzt. IBM bietet die Cloud-basierte Plattform „Fan Insight“ an, welche

---

18 Gudmundsson/Horton, S. 22.8.

19 Gudmundsson/Horton, S. 22.15.

20 Kempe et al., S. 249, 254.

21 Memmert/Lemmink et al., S. 2.

22 Rudenko, Big Data in Sports: Going for the Gold, https://insidebigdata.com/2017/06/04/big-data-sports-going-gold/ (zuletzt aufgerufen am 21.09.2018); Sands et al., S. S2-63.

das Fanverhalten vorhersagen soll.[23] Im Ergebnis soll die Auslastung der Sportstätte und der allgemeine Umsatz optimiert werden. Jedoch wird sich das Stadionerlebnis auch aus Kundensicht grundlegend verändern. Bereits bei der Ankunft am Stadion wird in Zukunft eine App den Stadionbesucher zum nächsten verfügbaren Parkplatz lotsen. Während des Spiels werden dann auf dem Smartphone Wiederholungen und alternative Sichten auf das Spielfeld verfügbar sein. Zudem wird der Besucher Getränke und Snacks mobil bestellen können, sodass er seinen Platz nicht verlassen muss.[24]

Im Folgenden werden einige Anwendungen der Digitalisierung und von Big Data in verschiedenen Sportarten, mit Fokus auf dem Fußball, exemplarisch vorgestellt, sodass klar wird, warum sich im Zusammenhang mit dem Einsatz von Big Data im Profisport von „Daten-Doping“ sprechen lässt.

1. Fußball

Mehr als 270 Millionen Menschen sind weltweit aktiv an Fußballspielen beteiligt.[25] Damit ist Fußball eine der beliebtesten und weitverbreitetsten Sportarten. Aufgrund der daraus resultierenden wirtschaftlichen Bedeutung wird immer nach Möglichkeiten der Optimierung gesucht.

Ein Paradebeispiel stellt der FC Midtjylland, ein Verein aus der dänischen ersten Liga (Superliga), dar. Dieser wurde im Sommer 2014 in „Moneyball“-Manier revolutioniert, nachdem er einen neuen Eigner bekam. So erhielten Erkenntnisse basierend auf den Daten und dem Modell des Unternehmens Smartodds, welches professionell auf Fußballspiele wettet, Einzug in den Betrieb der Profi-Mannschaft. Das Modell geht davon aus, dass, entgegen der allgemein bekannten Phrase, die Tabelle lügt.[26] Im Kern geht es zur Optimierung der Erfolgschancen darum, zu ermitteln,

---

23 IBM, Fan Insight, https://www.ibm.com/de-en/marketplace/fan-insight-for-sports-and-venues (zuletzt aufgerufen am 21.09.2018).

24 Kumar, 3 ways big data and analytics will change sports, https://www.ibmbigdatahub.com/blog/3-ways-big-data-and-analytics-will-change-sports (zuletzt aufgerufen am 02.10.2018).

25 FIFA 2006, S. 1.

26 Biermann, S. 93.

welche Mannschaft wie viele Torchancen hatte und von welcher Qualität diese waren. Die Mannschaft mit der besseren Chancenverteilung war, unabhängig vom Endergebnis, das bessere Team.[27] Zudem werden auch „Key Performance Indicators“, also zentrale Qualitäten, für jeden Spieler bestimmt und die grundsätzliche Taktik, unabhängig vom Spielstand immer weiter Torabschlüsse zu kreieren, vorgegeben.[28] Durch die Orientierung an dem Modell verändert sich die übliche Wahrnehmung der sportlichen Performance. Dies führt beispielsweise dazu, dass ein Trainer nicht auf Grund einer schlechten Tabellenposition oder eines schlechten Ergebnisses entlassen wird. Jedoch muss er sich gegebenenfalls auch bei gewonnenen Spielen rechtfertigen, sofern das Modell eine bessere Leistung prognostiziert hat.[29] Die Daten werden auch zur Absicherung von Spielertransfers verwendet. Ein internationales Vereinsranking vergleicht die Spielstärke und ermöglicht so, qualitativ passende Spieler für möglichst geringe Kosten zu finden.[30] Dadurch kann der relativ kleine FC Midtjylland datenbasiert quasi weltweit scouten. Die Technik zahlt sich aus. Der FC Midtjylland wurde 2015 und 2018 dänischer Meister.

Aber selbst auf Regionalliga-Ebene hält nun Big Data Einzug. Der Viertligist SG Wattenscheid 09 plant, die erste Mannschaft in eine GmbH auszugliedern und das Start-up Haalo als Teilhaber ins Boot zu holen. Haalo entwickelt einen Big-Data-Scout, der Millionen Leistungsdaten von Spielern, insbesondere von Talenten, analysiert. Der Verein soll das erste Versuchsfeld und erster Profiteur der Technik sein.[31] Bald werden alle Spiele und Trainings des Vereins gefilmt. Das Trackingsystem wird dazu genutzt werden, um potentielle Spieler zu analysieren und im Anschluss Zukunftsprognosen zu erstellen. Dadurch kann dann 13- oder 14-jährigen Spielern angedeutet werden, ob ein Leben als Profifußballer möglich erscheint, oder ob lieber auf einen konventionellen Beruf gesetzt werden sollte.[32] Im Endeffekt möchten aber natürlich die SG Wattenscheid 09,

---

27 Biermann, S. 94.

28 Biermann, S. 95.

29 Biermann, S. 95.

30 Biermann, S. 95.

31 Müllender, S. 54.

32 Müllender, S. 56.

indem sie ein Hotspot für Talente wird, und Haalo, indem es die Technik an andere Vereine verkauft, profitieren.[33]

Der FC Midtjylland und die SG Wattenscheid 09 sind jedoch längst nicht die Einzigen, die technikgestützt Transfers vornehmen. Die französisch-englische Firma Amisco/Prozone wertet jährlich über 9000 Fußballspiele aus und verkauft die generierten Ergebnisse zum Beispiel an die gesamte englische Premier League, die deutsche Nationalmannschaft und den FC Bayern München. Die Daten ermöglichen es, gezielt nach Spielern mit einem bestimmten Profil zu suchen.[34] Interessant ist dies vor allem hinsichtlich solcher Spieler, die in eher kleineren oder zweiten Ligen spielen.[35] Diese können Scouts oft nicht ausreichend abdecken. Jeden Spieler findet man dann im sog. Online-Recruiter. Dort werden die ermittelten Werte für verschiedenste Fähigkeiten des Spielers mit den Durchschnittswerten seiner Liga ins Verhältnis gesetzt. Dabei geht es zum Beispiel um die Passgenauigkeit, jeweils unterteilt nach Zonen, die gewonnenen Zweikämpfe oder die abgefangenen Bälle.[36]

Die Leistungsdichte auf der allerhöchsten Ebene des Profifußballs ist heutzutage vergleichsweise hoch. Dabei ist die individuelle physische und mentale Verfassung der Spieler Ansatzpunkt für den Einsatz von Big-Data-Technologien. Darüber hinaus verspricht Big Data aber auch strategische Vorteile bei der Bewertung der mannschaftlichen Leistung. Die Botschaft lautet: Big Data vermittelt Einblicke in bedeutungsvolle Zusammenhänge, die dem Gegner möglicherweise nicht bekannt sind bzw. die der Gegner möglicherweise nicht korrekt einordnen kann. Diese Zusammenhänge gehen dabei nicht als „Datenflut“ über die handelnden Personen nieder, sondern werden als konkrete Phänomene beschrieben, die die für die sportliche Umsetzung verantwortlichen Personen in ihre Überlegungen einbeziehen können. Ein Beispiel für einen solchen Zusammenhang, der durch Big Data vermittelt wird, ist das Phänomen des „Pa-

33 Müllender, S. 56.

34 Schrenk, S. 56.

35 Schrenk, S. 57.

36 Schrenk, S. 62.

ckings“. Hiermit werden die Aktionen bezeichnet, die bewirken, dass weniger Gegner zwischen dem Ball und dem gegnerischen Tor stehen.[37] Auf Basis dieser Methode wird untersucht, mit welcher Häufigkeit Gegner überspielt werden, das Überspielen von Gegnern durch das Anbieten als Anspielstation ermöglicht wurde, aber auch, wie viele Mitspieler durch einen Ballverlust aus dem Spiel genommen worden sind.[38] Dies wird mit einem spezifischen Wert gewichtet. Genauso kann gemessen werden, mit welcher Intensität ein Team überspielt worden ist und die Ballgewinne im offensiven wie im defensiven Bereich können analysiert werden.[39] Während der Fußball-Europameisterschaft 2016 wurde die Packing-Kennzahl der überspielten Gegner einem millionenweiten Fernseh-Publikum als Kriterium präsentiert, bei dem es im Gegensatz zu üblichen Parametern um Qualität statt Quantität ginge.[40] Auch wenn der mediale „Packing-Hype“ mittlerweile etwas abgeklungen ist, ist das Phänomen als Kennzahl in der statistischen Fußball-Analyse angekommen. Immerhin acht Bundesligisten nutzten die Methodik in ihren Analysen.[41]

Daneben bestehen weitere spannende Möglichkeiten. Eine etablierte Big-Data-Kennzahl im Profifußball ist auch der Wert „Expected Goals“, der sog. xG-Wert (bzw. xGA-Wert für Gegentore). Dieser Kennziffer liegt die Idee zugrunde, bestimmen zu können, mit welcher Wahrscheinlichkeit aus einem abgegebenen Torschuss ein Treffer wird.[42] Erheblichen Einfluss auf die Wahrscheinlichkeit hat zum Beispiel die Position auf dem Spielfeld, von der der Torschuss unternommen wird. Durch Voronoi-Diagramme hingegen kann die Raumkontrolle einer Mannschaft erfasst werden. In diesen wird jedem der 22 Spieler auf dem Fußballfeld ein Raum

---

37 Impect, https://www.impect.com/de/#idea (zuletzt aufgerufen am 01.10.2018).

38 Impect, https://www.impect.com/de/#idea (zuletzt aufgerufen am 01.10.2018).

39 Impect, https://www.impect.com/de/#idea (zuletzt aufgerufen am 01.10.2018).

40 Katzenberger, Hat jemand „Packing“ gesagt?, https://www.sueddeutsche.de/medien/diskussion-ueber-neue-fussball-kennzahl-hat-jemand-packing-gesagt-1.3034933 (zuletzt aufgerufen am 01.10.2018).

41 Niessen, Gibt es eigentlich noch „Packing“? 8 Bundesliga-Vereine schwören drauf, https://www.watson.de/sport/interview/458713925-gibt-es-eigentlich-packing-noch-8-bundesliga-vereine-schwoeren-drauf (zuletzt aufgerufen am 01.10.2018).

42 Biermann, Das Favre-Rätsel, https://www.11freunde.de/artikel/welche-spielidee-der-neue-bvb-trainer-hat (zuletzt aufgerufen am 01.10.2018).

zugeordnet. Diesen Raum kontrolliert er, da er diesen vor allen anderen Spielern erreichen kann. Für jede Mannschaft ergibt sich daraus ein Wert, der insbesondere für den Raum um und im gegnerischen Strafraum besonders aussagekräftig ist.[43] Ein weiterer Parameter erfasst das Pressing-Verhalten einer Mannschaft. Dazu wird gemessen, wie schnell die Spieler der gegnerischen Mannschaft nach einem eigenen Ballverlust angelaufen werden. Das Ergebnis spiegelt die Erfolgsquote im Pressing und die Aggressivität einer Mannschaft wieder.[44]

2. Formel 1

Dass der Motorsport besonders datengetrieben ist, liegt in der Natur der Sache. Im Gegensatz zu einem menschlichen Körper lässt sich die Maschine Rennwagen besonders gut und genau auslesen. Jedes noch so kleine Detail wird während des Trainings und des Rennens analysiert und in Realzeit interpretiert. Doch dies stellt auch eine Schwäche dar. Gehen Daten verloren oder wird die Software eines Rennstalls mit Malware infiziert, ist die Leistungsfähigkeit des Rennfahrers enorm beeinträchtigt.[45]

In der Formel 1 geht es um viel Geld. Dies liegt allerdings vor allem an den horrenden Kosten, die der Betrieb eines Rennstalls kostet. Nicht ohne Grund wird daher in der Formel 1 bald eine Budgetobergrenze eingeführt. Die großen Teams hoffen, dass diese bei 200 Millionen Euro liegen wird und nicht deutlich darunter.[46] Denn bei einem Rennstall ist alles teuer. Beispielsweise kostet jeder gefahrene Testkilometer im Schnitt ca. 1000 Euro. Doch Hilfe bietet die Digitalisierung. Testfahrten werden

---

43 Memmert/Raabe et al., S.19.

44 Memmert/Raabe et al., S.19.

45 Marr, The Risks Of Big Data In Sports, https://www.forbes.com/sites/bernardmarr/2017/04/28/the-big-risks-of-big-data-in-sports/#193010277c6f (zuletzt aufgerufen am 21.09.2018).

46 Schmidt, Budget-Deckel kommt 2019 als Testjahr, https://www.auto-motor-und-sport.de/formel-1/f1-kosten-obergrenze-budget-deckel-2019-testjahr/ (zuletzt aufgerufen am 21.09.2018).

durch Big-Data-Simulierungen ersetzt und die CAD-Technologie (computer-aided design) erleichtert die Konstruktion.[47] Interessanterweise begrenzt der Automobilweltverband FIA das Datenvolumen bei Aerodynamik-Simulationen.[48] Big Data hat jedoch nicht nur Einfluss auf die Finanzen. Auch der sportliche Erfolg hängt von der Arbeit der IT-Experten ab. Längst ist ein guter Fahrer nur noch eine überschaubare Voraussetzung für Erfolg. Die Bestimmung der Strategie, die Feineinstellung und Überwachung der Funktionalitäten des Wagens und die Überwachung der Kontrahenten erfolgen neben der Rennstrecke und parallel dazu in der heimischen Stallfabrik. Dort stehen Computer mit enormer Rechenleistung, auf die das Team während des Rennens zugreift.[49]

3. Weitere US-Sportarten

Auch in anderen Sportarten wird verstärkt auf Big Data gesetzt. Allen voran geschieht dies im Bereich der, traditionell Innovationen sehr zugänglichen, US-Sportarten. Die Dallas Cowboys begannen 2015 als erstes Team der amerikanischen Football-Liga (NFL) Virtual Reality zur Unterstützung ihres Trainings zu verwenden. Dazu werden Teile ihres Trainings mit Drohnen und 360-Grad-Kameras gefilmt. Die Trainer können so live und aus Spielersicht mitverfolgen, ob zentrale Spieler sich auf dem Feld richtig verhalten. Zudem können Spieler nachträglich in die Spielsituation versetzt werden, um Fehler zu besprechen.[50] Die Dallas Cowboys und mittlerweile mindestens 24 andere Teams kooperieren dazu mit STRIVR Labs. Diese rühmen sich, durch ihr Virtual-Reality-Produkt bei den Spielern die Reaktionszeit, die Fähigkeit zur Erkennung von Mustern und

---

47 Brümmer, Der Große Preis von Big Data 2015 – IT in der Formel 1, https://www.computerwoche.de/a/it-in-der-formel-1,3213160 (zuletzt aufgerufen am 21.09.2018).

48 Fédération Internationale de l'Automobile (FIA), S. 56 ff.

49 Brümmer, Der Große Preis von Big Data 2015 – IT in der Formel 1, https://www.computerwoche.de/a/it-in-der-formel-1,3213160 (zuletzt aufgerufen am 21.09.2018).

50 Archer, Cowboys to use virtual reality to help players in film study, http://www.espn.com/dallas/nfl/story/_/id/13029637/dallas-cowboys-use-virtual-reality-technology (zuletzt aufgerufen am 21.09.2018).

Geschwindigkeit, in der Entscheidungen getroffen werden, zu verbessern.[51] Die Cleveland Browns hingegen verwenden Trackingdaten, um verletzungsanfällige Spieler vor Rückfällen zu schützen.[52]

In der nordamerikanischen Basketball-Profiliga (NBA) sind alle Arenen mit sechs Kameras des Unternehmens STATS ausgestattet, welche die Bewegungen jedes Spielers und des Basketballs 25-mal pro Sekunde bestimmen.[53] Zudem enthält selbst die Trainingskleidung Sender. Ein Algorithmus erlaubt dann die Erfassung von plötzlichen Bewegungen und die Bestimmung der Kraft, Richtung und Neigung des Sportlers.[54] Die Golden State Warriors kamen als erstes Team der NBA mit Hilfe von Datenanalysen zu der simplen Erkenntnis, dass ein konsequentes Drei-Punkt-Spiel statistisch zu mehr Punkten führt. Der Jump-Short unter dem Korb ist zwar einfacher, jedoch im Ergebnis nicht sinnvoll. Im Jahr 2012 versuchten NBA-Teams im Durchschnitt 18,4 Drei-Punkt-Würfe, im Jahr 2017 waren es bereits 27.[55]

V. Verbot technischer Hilfsmittel im Profisport

Ein zentrales Verbot technischer Hilfsmittel ist vor nicht allzu langer Zeit gefallen. Das International Football Association Board (IFAB), ein internationales Gremium, welches Änderungen der Fußballregeln berät und beschließt, hat sein Regelwerk in Bezug auf den Einsatz elektronischer

---

51 STRIVR Labs, Inc., Press Release 14.12.2016, STRIVR Labs announces funding to expand VR training platform to include enterprise customers, https://www.strivr.com/wp-content/uploads/2017/01/strivr-labs-press-release-12-14-16.pdf (zuletzt aufgerufen am 21.09.2018).

52 Fischer, Wie Datenanalyse den Leistungssport verändert, https://www.welt.de/gesundheit/article153950153/Wie-Datenanalyse-den-Leistungssport-veraendert.html (zuletzt aufgerufen am 21.09.2018).

53 Brousell, 8 Ways Big Data and Analytics Will Change Sports, https://www.cio.com/article/2377954/data-management/data-management-8-ways-big-data-and-analytics-will-change-sports.html (zuletzt aufgerufen am 02.10.2018).

54 Fischer, Wie Datenanalyse den Leistungssport verändert, https://www.welt.de/gesundheit/article153950153/Wie-Datenanalyse-den-Leistungssport-veraendert.html (zuletzt aufgerufen am 21.09.2018).

55 Moll, Im Datenwahn, Frankfurter Allgemeine Sonntagszeitung, 11. März 2018, S. 40.

Kommunikation erst 2018 geändert. War nach Regel 04.4. a.F. der Einsatz irgendeiner Form von elektronischer Kommunikation durch Teamoffizielle noch unzulässig, sofern dies nicht in direktem Bezug zum Wohlbefinden oder zur Sicherheit der Spieler geschah, gilt dies nicht mehr länger. Vielmehr ist der Einsatz von elektronischen oder Kommunikationsgeräten durch Teamoffizielle nun auch zulässig, sofern dies zu Taktik- oder Coachingzwecken geschieht. Eingesetzt werden dürfen dabei nur kleine tragbare Mobilgeräte (z.B. Mikrofon, Kopfhörer, Ohrhörer, Mobiltelefon, Smartphone, Smartwatches, Tablet, Laptop).[56] Begründet wurde die Änderung von dem IFAB damit, dass eine Kommunikation in die und aus der technischen Zone fast nicht auszuschließen sei und ein Austausch von Informationen zu Taktik- oder Coachingzwecken oder zum Wohl der Spieler sinnvoll sei.[57] Die Begründung des IFAB offenbart eine gewisse Resignation, schwingt doch mit, ein Verbot technischer Hilfsmittel sei ohnehin nicht durchzusetzen. Nicht auszudenken, die WADA oder die NADA würde damit argumentieren, dass Doping erlaubt sei, da es ohnehin nicht zu verhindern sei. Ein ähnlicher Aufschrei bleibt für das Verbot technischer Hilfsmittel indes aus. Hier zeigt sich wiederum, dass die Ablehnung technischer Hinsicht jedenfalls nicht auf einem so breiten gesellschaftlichen Konsens basiert wie das Doping. Vielmehr wird der Profisport gerade aus gesellschaftlicher Perspektive stark mit dem Optimierungsgedanken verknüpft. Das sieht man auch am zweiten Teil der Begründung des IFAB, das einen Austausch von Informationen zu Taktik- oder Coachingzwecken ohne Weiteres als sinnvoll erachtet.

VI. Begründungen für das Verbot technischer Hilfsmittel im Profisport und Big Data

Die Begründungen für Dopingverbote im Profisport lassen sich durchaus auf das Verbot technischer Hilfsmittel übertragen.

---

56 The International Football Association Board (IFAB), S. 59.

57 The International Football Association Board (IFAB), S. 157.

1. Chancengleichheit

Auch im Profisport wird das Verbot technischer Hilfsmittel mit dem Argument der Chancengleichheit begründet. Zum Beispiel betont das IFAB in der Einführung zu den Spielregeln der Fußballsaison 2018/19 „[die] bedeutende Stärke [, dass die Spielregeln] „für jedes Spiel in jeder Konföderation, in jedem Land, in jeder Stadt und in jedem Dorf weltweit gelten".[58] Werden nun technische Hilfsmittel zugelassen, so werden diese aus finanziellen, technischen und organisatorischen Gründen nicht gleichermaßen überall eingesetzt werden können. Auch wenn die Regeln die technischen Hilfsmittel überall zuließen, verändert die tatsächliche Verfügbarkeit technischer Hilfsmittel den Charakter des Spiels.

Ausgehend vom Moneyball-Narrativ könnte man in Big-Data-Anwendungen auch eine Möglichkeit sehen, der wachsenden Ungleichheit im Sport Herr zu werden. Demnach bringt Big Data Chancengleichheit in den Wettkampf, der längst mehr durch Geld als durch ein faires Messen der sportlichen Fähigkeiten entschieden wird. Doch ist diese Hypothese kritisch zu hinterfragen. So stellen Big-Data-Anwendungen letztlich ein weiteres Instrument zur Optimierung der sportlichen Leistung dar. Sie sind insofern vergleichbar mit den bisher verfügbaren Maßnahmen. Auf die lange Sicht gesehen werden eher finanzstarke Akteure sich durch weitere zur Verfügung stehende Mittel mehr Vorteile verschaffen können.

Bereits jetzt besteht ein großer Kritikpunkt am Einsatz technischer Hilfsmittel wie Torlinientechnik, VAR (Video Assistant Referee) etc. darin, dass alle Stadien mit der gleichen Technik ausgerüstet werden müssen. Diese Kosten tragen zu einem großen Teil die Vereine.[59] Langfristig könnten sich die finanzstarken Akteure hierdurch einen weiteren Vorteil verschaffen. Am Ende gewinnt dann nicht mehr, wie im Beispiel von „Moneyball", der Underdog, sondern der „Big Player".

---

58 The International Football Association Board (IFAB), S. 11.

59 Spiegel Online, Bundesliga verzichtet auf Torlinientechnik, http://www.spiegel.de/sport/fussball/bundesliga-fuehrt-torlinientechnologie-vorerst-nicht-ein-a-960412.html (zuletzt aufgerufen am 20.09.2018).

2. Medizinische Gründe

Medizinische Gründe hingegen sprechen bislang nur sehr bedingt gegen den Einsatz technischer Hilfsmittel im Profisport. Auswirkungen des „Daten-Dopings“ sind nicht mit den Gefahren des Missbrauchs von Pharmazeutika zu vergleichen. Vielmehr führen IFAB und DFB den Gesundheitsschutz als einen der Gründe für die Nutzung von technischen Hilfsmitteln im Fußball an.[60] In Zukunft könnte sich dies jedoch ändern. Vor allem ist nicht auszuschließen, dass psychische Auswirkungen einer „Dauerüberwachung“ von Spitzenathleten gesundheitsschädlich sein können.

Die Flut an gesammelten Daten lässt den Athleten, auch in Teamsportarten, gläsern werden. Was die gemeine Bevölkerung bei der Verwendung von sozialen Netzwerken fürchtet, wird für Sportler Realität.[61] Der Arbeitgeber, zum Beispiel ein Verein im professionellen Sport, überwacht über Pulsmesser und Blutwertbestimmungen dezidiert die Funktionsfähigkeit des Organismus. Ob der Sportler am Abend zuvor noch ausgiebig Zeit in einem Fast-Food-Restaurant verbracht hat oder während der Sommerpause seinen Trainingsplan eingehalten hat, lässt sich so unproblematisch überwachen.

3. Eigenart des Sports

Zudem lässt sich die Ablehnung des Einsatzes technischer Hilfsmittel im Sport auch mit der Eigenart des Sports rechtfertigen. So ist zum Beispiel im Fußball die Verwendung technischer Hilfsmittel zur Unterstützung der Schiedsrichter auf heftigen Widerstand gestoßen. Gegner verweisen auf die Kultur des Fußballs beziehungsweise des sportlichen Wettkampfs im Generellen. So lebe der Sport gerade von der Unvollkommenheit des Menschen, die sich in einem verfehlten Torschoss oder einer Fehlentscheidung des Schiedsrichters äußert. Anders ausgedrückt: „Der Fußball

---

60 The International Football Association Board (IFAB), S. 157; Sportschau, Elektronische Kommunikation jetzt auch in der Bundesliga, https://www.sportschau.de/fussball/bundesliga/bundesliga-technische-hilfsmittel-erlaubt-100.html (zuletzt aufgerufen am 20.09.2018).

61 Siehe zu den sozialen Netzwerken das Dossier „Big Social Data“ (F.).

soll menschlich bleiben“, so Michel Platini, ehemaliger Präsident des europäischen Verbandes UEFA.[62]

VII. Fazit

Im Ergebnis steht fest, dass Big Data massive Vorteile bietet. Die Auswertung der vorhandenen Daten gestaltet sich jedoch mitunter als schwierig. Insbesondere Sportarten mit komplexen Abläufen und, aus mathematischer Sicht, vielen Variablen lassen sich nur schwer vollständig auslesen. Geht es nicht nur um die athletischen Werte eines einzelnen Spielers, sondern um Teamtaktik und die Interaktion der Teammitglieder untereinander, ist enorme Rechenleistung und umfassendes Know-How erforderlich. Big-Data-Anwendungen stellen derzeit lediglich eine Hilfe zur Entschlüsselung von Spielideen und Taktik dar. Nicht ausreichend ist es, zum Beispiel im Fußball, lediglich einen hohen xG-Wert oder maximal möglichen Ballbesitz erzielen zu wollen, auch wenn dies mathematisch sinnvoll ist. Die Fokussierung auf den Ballbesitz hat auch dem Bundestrainer der deutschen Nationalmannschaft Joachim Löw bei der Fußball-WM 2018 nicht geholfen. Man muss in der Lage sein, die Daten zu interpretieren. Beispielweise bedeutet eine schlechte Passquote nicht automatisch, dass der Spieler schlecht ist. Vielmehr kann es sein, dass der Trainer von diesem Spieler bewusst riskante Pässe fordert. Diese werden jedoch häufiger abgefangen.[63]

Big Data stellt jedoch in jedem Fall einen Eingriff in die Natürlichkeit des Sports dar. Der Sportler an sich und die entsprechenden Sportgeräte reichen nicht mehr aus, um erfolgreich zu sein. Dadurch entsteht eine Art Materialschlacht, aus der die großen Player letztendlich als Sieger hervorgehen werden. Denn die Beschaffung, Auswertung und Interpretation von Daten kostet Geld. Parallelen lassen sich zu vielen Sportarten ziehen. Beispielsweise wurden im Schwimmsport 2009 Ganzkörper-Glatthautschwimmanzüge, die immer neue Fabelzeiten generierten, von der

---

62 Klappenbach/Teuffel, Warum sind technische Hilfsmittel so umstritten?, https://www.tagesspiegel.de/sport/fussball-wm2010/fehlentscheidungen-warum-sind-technische-hilfsmittel-so-umstritten/1871106.html (zuletzt aufgerufen am 20.09.2018).

63 Schrenk, S. 63.

FINA (Fédération Internationale de Natation), dem Dachverband aller nationalen Sportverbände für Schwimmen, verboten. Beim Schwimmen hatten die Anzüge zu immer größeren Verwerfungen geführt, da der Sieg zum Teil vom Sponsor und dessen aktuellen Entwicklungsstand abhing. Sportler aus Ländern ohne entsprechende Finanzierung hatten gar keine Chance mehr. In diesem Zusammenhang wurde bereits von technologischem Doping gesprochen.[64] Die Chancengleichheit kann extrem gestört sein. Jedoch kann man nicht alle Situationen über einen Kamm scheren. Im Fußball sind verschiedenste Daten und Analysen relativ leicht und für die Vereine auch sehr günstig zu haben. In jedem Fall stehen die Kosten in keinem Vergleich zu den horrenden Ablösesummen.[65] Im Fußball wird die Chancengleichheit schon lange durch ganz andere Maßnahmen, wie zum Beispiel die Verteilung der TV-Einnahmen, untergraben.

Insofern geht mit der Digitalisierung und der Verbreitung von Big Data eine tiefgreifende Veränderung des Sports einher. Daher ist es durchaus sinnvoll, sich Gedanken über eine Limitierung der technologischen Möglichkeiten zu machen. Hier spielt insbesondere der Gesichtspunkt der Chancengleichheit eine Rolle. Zu bedenken ist jedoch, dass am Ende immer der Athlet seine Leistung abrufen muss. Diese direkt kann Big Data, im Gegensatz zu traditionellem Doping, nicht beeinflussen. Big-Data-Anwendungen wirken sich insbesondere auf die Vorbereitung, also das athletische und taktische Training, und bei der Überwachung des Leistungsstandes eines Sportlers, aus. Ob in einigen Jahren eine Neubewertung von Nöten ist, wird die Zukunft zeigen.

Literaturnachweise

Biermann, Moneyball im Niemandsland, 11Freunde #163, Juni 2015, S. 90-96.

Camus, France Football N°613, 1957.

---

64 Philippsen, Warum sind alle Schwimmer schnell – nur die Deutschen nicht?, http://www.faz.net/aktuell/sport/olympia-2008/wassersport/leser-fragen-faz-net-antwortet-3-warum-sind-alle-schwimmer-schnell-nur-die-deutschen-nicht-1678829.html (zuletzt aufgerufen am 04.10.2018).

65 Schrenk, S. 61.

Fédération Internationale de l'Automobile (FIA), 2018 FORMULA ONE SPORTING REGULATIONS, 17 July 2018.

FIFA 2006, FIFA Big Count 2006.

FIFA 2018, FIFA Anti-Doping Regulations 2018 edition.

Gudmundsson/Horton, Spatio-Temporal Analysis of Team Sports, ACM Computing Surveys, Vol. 50, No. 2, Article 22, 2017.

Kempe/Grunz/Memmert, Detecting tactical patterns in basketball: Comparison of merge self-organising maps and dynamic controlled neural networks, European Journal of Sport Science 2015, S. 249-255.

Lamoreaux, Baseball in the late nineteenth century: The source of its appeal, Journal of Popular Culture 11, 1977, S. 597-613.

Memmert/Lemmink/Sampaio, Current Approaches to Tactical Performance Analyses in Soccer Using Position Data, Sports Medicine 2017, S. 1-10.

Memmert/Raabe/Knyazev/Franzen/Zekas/Rein/Perl/Weber, Innovative Leistungsindikatoren im Profifußball auf der Basis von Positionsdaten, Impulse 2016, 2, S. 14-21.

Müllender, Revolution an der Lohrheide, 11Freunde #203, Oktober 2018, S. 52-56.

Nationale Anti Doping Agentur Deutschland, Nationaler Anti-Doping Code (NADC 2015), 2015.

Pawlenka, Ethik, Natur und Doping im Sport, Sportwissenschaft 2012, S. 6-16.

Sands/Kavanaugh/Murray/McNeal/Jemni, Modern Techniques and Technologies Applied to Training and Performance Monitoring, International Journal of Sports Physiology and Performance 2017, S2-63-S2-72.

Schrenk, Ist Fußball etwa doch Mathematik? Ein Gespräch mit dem Datenscout Jannis Scheibe, in: Big Data – Das neue Versprechen der Allwissenheit, Geiselberger/Moorstedt Berlin 2013.

The International Football Association Board (IFAB), Spielregeln 2018/19, gültig seit dem 1. Juni 2018.

Autorenverzeichnis

Philip Bitter, Wissenschaftlicher Mitarbeiter am Institut für Informations-, Telekommunikations- und Medienrecht der Universität Münster. Studium der Rechtswissenschaften in Münster.

Henning Brockmeyer, Ass.-Jur., Wissenschaftlicher Mitarbeiter am Institut für Informations-, Telekommunikations- und Medienrecht der Universität Münster. Studium der Rechtswissenschaften in Passau, Referendariat in Münster.

Dr. Nicolai Culik, ehemals Wissenschaftlicher Mitarbeiter am Institut für Informations-, Telekommunikations- und Medienrecht der Universität Münster und momentan Referendar in Berlin. Studium der Rechtswissenschaften in Konstanz, Lyon und Münster.

Christian Döpke, Rechtsanwalt, LL.M., LL.M., ehemals Wissenschaftlicher Mitarbeiter am Institut für Informations-, Telekommunikations- und Medienrecht der Universität Münster. Studium der Rechtswissenschaften in Osnabrück, Hannover und Oslo, Referendariat am OLG Oldenburg.

Lukas Forte, ehemals Studentische Hilfskraft am Institut für Informations-, Telekommunikations- und Medienrecht der Universität Münster. Studium der Rechtswissenschaften in Münster.

Dr. Tim Jülicher, B.A., Rechtsreferendar beim Oberlandesgericht Düsseldorf. Zuvor wissenschaftlicher Mitarbeiter am Institut für Informations-, Telekommunikations- und Medienrecht der Universität Münster. Studium der Politik- und Rechtswissenschaften in Münster.

Dr. Barbara Kolany-Raiser, Wissenschaftliche Mitarbeiterin am Institut für Informations-, Telekommunikations- und Medienrecht der Universität Münster. Studium der Rechtswissenschaften in Graz und Madrid.

Matthias Möller, ehemals Studentische Hilfskraft am Institut für Informations-, Telekommunikations- und Medienrecht der Universität Münster. Studium der Rechtswissenschaften in Münster.

Maurice Niehoff, Ass.-Jur., Wissenschaftlicher Mitarbeiter am Institut für Informations-, Telekommunikations- und Medienrecht der Universität Münster. Studium der Rechtswissenschaften in Münster, Referendariat in Münster.

Tristan Radtke, Studentische Hilfskraft am Institut für Informations-, Telekommunikations- und Medienrecht der Universität Münster. Studium der Rechtswissenschaften in Münster.

Christian Straker, Ass.-Jur., Wissenschaftlicher Mitarbeiter am Institut für Informations-, Telekommunikations- und Medienrecht der Universität Münster. Studium der Rechtswissenschaften in Münster, Referendariat in Essen.

Tristan Julian Tillmann, Ass.-Jur., Wissenschaftlicher Mitarbeiter am Institut für Informations-, Telekommunikations- und Medienrecht der Universität Münster. Studium der Rechtswissenschaften in Münster und Ferrara, Referendariat in Münster.

Steffen Uphues, Wissenschaftlicher Mitarbeiter am Institut für Informations-, Telekommunikations- und Medienrecht der Universität Münster. Studium der Rechtswissenschaften in Münster.

Verena Vogt, Wissenschaftliche Mitarbeiterin am Institut für Informations-, Telekommunikations- und Medienrecht der Universität Münster. Studium der Rechtswissenschaften in Münster.

Nils Wehkamp, B.Sc., Wissenschaftliche Hilfskraft am Institut für Informations-, Telekommunikations- und Medienrecht der Universität Münster. Studium der Wirtschafts- und Rechtswissenschaften in Münster, zuvor Studium der Wirtschaftsinformatik in Stuttgart.

Lucas Werner, ehemals Studentische Hilfskraft am Institut für Informations-, Telekommunikations- und Medienrecht der Universität Münster. Studium der Rechtswissenschaften in Münster.

Phänomene des Big-Data-Zeitalters

Thomas Hoeren (Hrsg.)

Der vorliegende Sammelband widmet sich wichtigen Fragestellungen rund um den Begriff Big Data und berücksichtigt dabei das Zusammenspiel mit der Künstlichen Intelligenz und der Industrie 4.0. Er setzt sich zusammen aus einzelnen Dossiers, welche im Rahmen des ABIDA-Projekts verfasst wurden und Sachverhalte spezifischer Lebensbereiche vor allem rechtlich bewerten.

Das ABIDA-Projekt wird vom Bundesministerium für Bildung und Forschung gefördert und forscht zu gesellschaftspolitischen Auswirkungen des Einsatzes von Big-Data-Anwendungen. Aufgrund der interdisziplinären Ausrichtung des Projekts enthalten die Dossiers je nach Kontext ökonomische, soziologische, politologische oder ethische Implikationen.

Prof. Dr. Thomas Hoeren ist Direktor des Instituts für Informations-, Telekommunikations- und Medienrecht der Universität Münster.

23,60 €
ISBN 978-3-8405-0194-4