Die digitale Transformation in Institutionen des kulturellen Gedächtnisses

Antworten aus der Informationswissenschaft

Herausgegeben von **Stephan Büttner**

Soziale Netzwerke und Ethik: Problemdiagnose und Schlussfolgerungen

Hermann Rösch
Institut für Informationswissenschaft, Technische Hochschule Köln
hermann.roesch@th-koeln.de

Abstract:

Die Auseinandersetzung mit Sozialen Netzwerken unter ethischen Gesichtspunkten hat nicht zum Ziel, deren Funktionalität und Gebrauchswert grundsätzlich in Abrede zu stellen. Stattdessen geht es darum, Problemfelder zu identifizieren, einen Anstoß zu deren Beseitigung zu geben und Missbrauch grundsätzlich zu erschweren. Ethisch problematische Praktiken Sozialer Netzwerke beziehen sich vor allem auf die Grundwerte Datenschutz und Privatheit, auf die partielle Verschleierung der Grenze zwischen öffentlicher und privater Sphäre sowie auf Hassreden, Desinformation und Fake News. Zu fordern ist, dass die Geschäftspraktiken transparent gemacht werden, Nutzer Zugriff auf die über sie gespeicherten Daten erhalten und gestufte Opt-out-Funktionen angeboten werden. Darüber hinaus muss der Staat in der Informationsgesellschaft im Rahmen staatlicher Daseinsvorsorge allen Bürgerinnen und Bürgern die Chance zu geben, in ausreichendem Maße Informationskompetenz zu erwerben, um u.a. die Funktionsweise sowie die Vor- und Nachteile Sozialer Netzwerke angemessen einschätzen zu können.

1. Ausgangslage

Im Folgenden stehen solche Sozialen Netzwerke im Mittelpunkt, die ihren Nutzern im Internet durch Vernetzung die Chance zum Austausch von Alltagserfahrungen, Meinungen und Informationen in Form von Text-, Bild-, Film- oder Tonnachrichten geben. Strukturell bestehen der-

artige Soziale Netzwerke zunächst aus den individuellen Profilen, der Liste anderer Nutzer, mit denen „Freundschaftsbeziehungen“ geknüpft worden sind und der Möglichkeit, Nachrichten blogähnlich zu posten bzw. untereinander auszutauschen. Innerhalb des Netzwerkes besteht die Möglichkeit, nach anderen Nutzern zu suchen und gegebenenfalls eine Freundschaftsanfrage zu stellen, die bei einigen Anbietern vom Adressaten akzeptiert werden muss, damit es zu einer gegenseitigen Aufnahme in die jeweiligen Kontakt-Netzwerke kommt. Ist dies geschehen, können miteinander „befreundete“ Nutzer ihre jeweiligen Profile einsehen und erhalten die Mitteilungen und Statusmeldungen des bzw. der anderen. Darüber hinaus besteht die Möglichkeit, diese Mitteilungen gegenseitig zu kommentieren und zu bewerten. Bei Facebook geschieht dies z.B. durch Anklicken des sog. Like-Buttons.

Die Nutzer haben die Option, den Zugriff auf die über ihr Profil zugänglichen Informationen zu steuern. Ihr Name und ihr Profilbild sind grundsätzlich öffentlich; alle anderen Informationen können sie für die Öffentlichkeit sperren und nur ihrem Freundesnetzwerk zugänglich machen. Bei der Beschreibung des eigenen Profils werden Aussagen abgefragt zu Alter, Geschlecht, Wohn- und früheren Aufenthaltsorten, Ausbildungsgang, Beruf, Mitgliedschaft in Institutionen, Hobbies, Vorlieben usw. Die Betreiber ermuntern ihre Nutzer dazu, die Profilbeschreibung so ausführlich wie möglich zu gestalten ohne im Einzelnen vorzuschreiben, dass die Kategorien ausgefüllt werden müssen. Pflicht ist es allerdings, den Namen anzugeben und ein Bild einzustellen. Facebook z.B. verlangt, dass der richtige Name angegeben wird. Diese Vorschrift wird jedoch nicht selten umgangen.

Zu den beliebtesten Anbietern Sozialer Netzwerke zählen Facebook, Google+, Xing, LinkedIn und Twitter. Facebook ist das weltweit größte Netzwerk mit 2 Milliarden Nutzern pro Monat (2017). Es wird vor allem im privaten Bereich genutzt. Allerdings besteht auch für Unternehmen die Möglichkeit, ein Facebook-Profil anzulegen und auf diese Weise Online-Marketing zu betreiben. Zudem können Künstler, Vereine, Interessenverbände, Behörden und Institutionen Fanseiten anlegen und so über Facebook für sich werben, Nachrichten verbreiten und sich vernetzen. Darüber hinaus besteht die Möglichkeit, themen- oder interessenspezifische Gruppen einzurichten. Diese können offen für alle Interessenten sein oder sich nur an ein ausgewähltes Publikum richten.

Google+ ist sowohl hinsichtlich der Funktionalitäten als auch des Zielpublikums vergleichbar mit Facebook. Der Unterschied besteht allerdings darin, dass die Kontaktaufnahme unidirektional erfolgt. Zur Herstellung einer Verbindung ist also keine Bestätigung seitens des Adressaten notwendig. Zwar wird Google+ im Unterschied zu Facebook in die Google-Suche eingebunden, doch kann das Angebot hinsichtlich der Nutzerzahlen bei weitem nicht mit dem Marktführer Facebook konkurrieren. Twitter ist anders ausgerichtet als Facebook und Google+. Es handelt sich bei Twitter um eine Microblogging-Plattform. Nutzer können Nachrichten von max. 280 Zeichen versenden. Die Vernetzung erfolgt unidirektional, d.h. eine Bestätigung ist wie bei Google+ nicht notwendig.

Weitere soziale Netzwerke wie Pinterest, Instagram, LinkedIn oder Xing mit teilweise unterschiedlichen Schwerpunkten ließen sich nennen. In den einschlägigen Statistiken wird Facebook eindeutig als Marktführer ausgewiesen und der Marktanteil weltweit mit ca. 75% angegeben.[1] Die Marktdominanz bei Sozialen Netzwerken ist zwar nicht so ausgeprägt wie bei Suchmaschinen, doch verfügt Facebook ebenso wenig über einen ernsthaften Konkurrenten wie Google bei den Suchmaschinen. Facebooks Marktführerschaft ist der Grund dafür, dass sich Praxisbeispiele im Folgenden vorwiegend auf das von Mark Zuckerberg erst 2004 gegründete Unternehmen beziehen.

Ethisch problematische Praktiken Sozialer Netzwerke beziehen sich vor allem auf die Grundwerte Datenschutz und Privatheit, auf die partielle Verschleierung der Grenze zwischen öffentlicher und privater Sphäre sowie auf Hassreden, Desinformation und Fake News. Daneben verweisen Kulturkritiker auf zahlreiche weitere negative Effekte. Für Simanowski etwa ist die „Facebook-Gesellschaft“ geprägt von einem Selbstdarstellungsimperativ, der narzisstische, exhibitionistische und voyeuristische Tendenzen in höchst bedenklicher Weise verstärkt.[2] Darüber hinaus führe die ständige Mitteilung des erlebten Augenblicks zum Verlust der Gegenwart sowie zum Verlust reflexiver Welt- und Selbstwahrnehmung.[3]

1 Vgl. Statcounter 2018.
2 Vgl. Simanowski 2016: 32, 34.
3 Vgl. Simanowski 2016: 15.

2. Datenschutz und Privatheit

Soziale Netzwerke beruhen auf einem ähnlichen Geschäftsmodell wie Suchmaschinen. Die Nutzer können die angebotenen Dienstleistungen vermeintlich kostenlos in Anspruch nehmen und sich mit ihren Profilen präsentieren, mit beliebig vielen anderen Nutzern der jeweiligen Plattform vernetzen sowie Nachrichten, Bilder, Filme usw. untereinander austauschen und bewerten. Als Gegenleistung erhalten die Betreiber i.d.R. das Recht, alle Inhalte für die eigenen Zwecke kommerziell auszuwerten oder an Geschäftspartner bzw. staatliche Behörden weiterzuleiten.

Die grundsätzlich positive Funktion sozialer Netzwerke besteht darin, Gleichgesinnte und Freunde im Netz aufzuspüren, um mit ihnen in Kontakt treten zu können. Facebook bietet dazu die Möglichkeit an, die E-Mailkontakte des eigenen E-Mailkontos zu kopieren und mit den E-Mail-Adressen der Facebook-User zu vergleichen. Auf dieser Grundlage werden dann Vorschläge für Freundschaftsanfragen unterbreitet. Allerdings werden auch die E-Mail-Adressen und Daten solcher Personen gespeichert, die nicht Mitglied von Facebook sind.

Dies ist nicht die einzige Praxis, die dazu führt, dass Facebook an Daten von Nicht-Nutzern kommt. Beim Besuch einer Facebook-Seite wird unabhängig davon, ob es sich um ein Facebook-Mitglied handelt oder nicht, im Browser ein Cookie platziert, das Informationen über die angesteuerten Webseiten speichert. Jedes Mal, wenn die entsprechende Person eine Seite aufruft, auf der Facebooks Like- bzw. Share-Button enthalten ist, werden die über das Cookie gespeicherten Navigationshistorien von Facebook ausgelesen, unabhängig davon, ob der Button angeklickt worden ist.[4] Immerhin 11% aller Webseiten (Stand 2018) haben den Like- bzw. Share-Button von Facebook eingebunden.[5]

Nutzer geben auf den Sozialen Netzwerken persönliche Daten nicht nur durch die mehr oder weniger ausführliche Selbstbeschreibung im Rahmen der vorgeschlagenen Kategorien bei der Beschreibung ihres Profils preis (Beruf, Hobbies, Vorlieben usw.). Eine wichtige Rolle in diesem Zusammenhang spielen die Like- und Share-Buttons. Im Unterschied zu anderen Netzwerken, die z.T. auch die Möglichkeit bieten,

4 Vgl. Facebook darf Daten über Nichtmitglieder sammeln 2016:
5 Vgl. Usage of social widgets for Websites 2018.

abstufende Bewertungen abzugeben (z.B. bis zu drei oder fünf Sterne) bietet Facebook nur die Möglichkeit, ein positives Votum („Like") abzugeben. Einen Dislike-Button wie z.B. bei Youtube gibt es dort hingegen nicht. Durch das Anklicken des Like- oder Share-Buttons werden die Nachrichten von Freunden, Ereignisse, Werbeauftritte oder Selbstdarstellungen von Gruppen, Unternehmen oder Produkten bestätigt bzw. positiv bewertet. Aus Sicht der Nutzer haben diese Aktivitäten die Funktion, die Vernetzung über die Bestätigung gemeinsamer Vorlieben zu verstärken und damit das Zugehörigkeitsgefühl zur eigenen Gruppe zu bestätigen. Für Unternehmen, Werbetreibende und Interessenvertreter aller Art hingegen spielen Like- und Share-Buttons eine zentrale Rolle im Rahmen des Social Media Marketings. Wird nämlich der Button auf Produkt-, Unternehmens- oder sonstigen Werbewebseiten von einem Facebook-Mitglied angeklickt, bedeutet dies, dass diese Seite allen seinen Freunden empfohlen wird. Für die Betreiber der Netzwerke wiederum werden die individuellen Nutzerprofile durch die Empfehlungen über Like- oder Share-Buttons fortwährend aktualisiert und erheblich angereichert. Dies verbessert die personalisierte Werbung und die Aussagekraft der Nutzerprofile insgesamt, die an Partner weiterverkauft werden. Besonderen ökonomischen Reiz gewinnen die von Facebook zusammengestellten Persönlichkeitsprofile, da sie in hohem Umfang mit den Klarnamen verbunden sind. Auch wenn einige Nutzer die Pflicht zur Angabe des richtigen Namens umgehen, ist doch der allergrößte Teil der Profile mit den zutreffenden Namen verknüpft.

Eine wachsende Rolle in den Sozialen Netzwerken spielt der Upload von Bildern. Es hat seinen besonderen Reiz, durch „Selfies" und Momentaufnahmen Alltagserlebnisse und kuriose Begebenheiten zu dokumentieren und die Freunde des Netzwerkes daran teilhaben zu lassen. Schon vor einigen Jahren bot Facebook seinen Nutzern an, auf Fotos Freunde zu identifizieren und durch automatische Analysetools nach groben Kategorien zu erschließen. Anschließend können Gesichter und Namensnennungen auf älteren Fotos abgeglichen werden. Bei der automatischen Gesichtserkennung werden biometrische Verfahren eingesetzt, die mittlerweile über eine hohe Zuverlässigkeit verfügen. In den meisten europäischen Ländern ist dafür jedoch die Zustimmung der

abgebildeten Personen notwendig. Daher bietet Facebook auf Druck hin diese Funktionen in Europa zurzeit nicht an.[6] In den USA werden hingegen alle hochgeladenen Bilder mit einer Gesichtserkennungssoftware analysiert. Facebook sieht darin einen Beitrag zur Verbesserung der Privatsphäre seiner Nutzer, denn diese werden automatisch benachrichtigt, wenn sie auf einem Bild identifiziert werden, das ihnen bislang nicht bekannt war.[7] Dieser Dienst wird in den USA grundsätzlich eingesetzt, Nutzer können ihn allerdings über eine Opt-Out-Funktion abschalten. Für die Nutzerprofile bietet Gesichtserkennung weiteres wichtiges Anreicherungspotential. Unter Gesichtspunkten des Datenschutzes sind diese Praktiken äußerst bedenklich. Niemand hat unter Kontrolle, wann er per Zufall im Alltag durch Dritte mit dem Smartphone, dem Tablet oder einer gängigen Digitalkamera im Hintergrund mit fotografiert wird, ganz zu schweigen von heimlichen und unerlaubten Aufnahmen, die mittlerweile auch per Drohne gemacht werden können. Die Chance, dass diese Fotos in nennenswertem Umfang in Soziale Netzwerke hochgeladen werden, ist hoch. Allein Facebook verfügt mit seinen 2 Milliarden Nutzern monatlich über eine kritische Masse. Wenn diese Fotos dann ausnahmslos mit Gesichtserkennungssoftware analysiert würden, ließen sich personenbezogene Daten in äußerst besorgniserregendem Umfang rekonstruieren.

Weitere Probleme hinsichtlich des Datenschutzes und des Schutzes von Privatheit ergeben sich dadurch, dass der Messaging-Dienst WhatsApp 2014 durch Facebook übernommen wurde. Bei WhatsApp handelt es sich um einen beliebten Dienst, der es Nutzern von Mobiltelefonen erlaubt, ohne direkte Kosten Textnachrichten, Bilder, Videos oder Tondokumente im bilateralen Austausch oder in der definierten Gruppe zu versenden. Auch das internetbasierte Telefonieren ist seit einiger Zeit möglich. Mit der Zustimmung zu den Datenschutzbedingungen müssen Nutzer, wenn sie das Funktionsangebot in zufrieden stellendem Umfang nutzen wollen, WhatsApp das Recht einräumen, die Telefonnummern ihrer Gesprächspartner und weitere Daten wie Zeitpunkt und Dauer der Kontakte oder den Standort weiterzugeben. Die Weitergabe erfolgt in erster Linie an den Mutterkonzern Facebook. Verbraucherschützer

6 Vgl. Conrad 2016.
7 Vgl. Reuter 2017.

bemängeln, dass auf diese Weise personenbezogene Daten von WhatsApp-Nutzern an Facebook gelangen, selbst wenn diese keine Facebook-Nutzer sind. Darüber hinaus werden die Telefonnummern von Dritten an Facebook weitergeleitet, die in den Adresslisten von WhatsApp-Nutzern gespeichert sind, ohne dass die Betroffen zugestimmt haben.[8] In Deutschland wurde WhatsApp 2017 gerichtlich untersagt, personenbezogene Daten an Facebook weiterzugeben. Das Verfahren ist noch nicht abgeschlossen.

Besondere Brisanz gewinnt die ungeheure Kumulation personenbezogener Daten durch Facebook auch unter dem Aspekt, dass Polizeibehörden und Nachrichtendienste darauf zugreifen. Insbesondere in totalitären und demokratiefeindlichen Regimen führt dies dazu, dass Fotos, Namen und Persönlichkeitsprofile von Dissidenten zu Zwecken der politischen Verfolgung genutzt werden. In der Türkei z.B. wurden Anfang 2018 über 600 Personen unter dem Vorwurf der Terrorpropaganda festgenommen, weil sie sich in Sozialen Netzwerken kritisch zur türkischen Militäroffensive in Syrien geäußert hatten.

Soziale Netzwerke sind ebenso wenig wie Suchmaschinen daran interessiert, ihre Nutzer über die reale Bedeutung und die Folgen der Sammlung und Auswertung ihrer personenbezogenen Daten nachhaltig aufzuklären. In der Datenrichtlinie von Facebook z.B. finden sich zum einen zahlreiche unkonkrete und unspezifische Formulierungen wie: „Für die in dieser Richtlinie beschriebenen Zwecke kann Facebook Informationen intern innerhalb seiner Unternehmensgruppe oder mit Dritten teilen." Wer diese Dritten sind und worin genau die Zwecke bestehen, wird nicht erläutert. Wer sich der zeitraubenden Lektüre dieser Richtlinie tatsächlich unterzieht, erfährt, dass Facebook zur Anreicherung der Persönlichkeitsprofile Daten auch bei externen Unternehmen erwirbt: „Wir erhalten von Drittpartnern Informationen über dich und deine Aktivitäten auf und außerhalb von Facebook… "[9] Zum Umgang mit den Daten in Facebooks Firmenimperium heißt es ferner: „Wir erhalten Informationen über dich von Unternehmen, die sich im Besitz von Facebook befinden oder von diesem betrieben werden, im Einklang mit deren Nutzungsbedingungen und Richtli-

8 Vgl. Was Facebook mit ihrem WhatsApp-Daten macht 2017.
9 Facebook 2016.

nien.“ [10] Dass dazu auch WhatsApp und Instagram gehören, ist einer Unterseite zu entnehmen, auf die man über einen „Erfahre mehr“-Link gelangt.“ Mit der konkludenten Zustimmung zu den Nutzungsbedingungen und der Datenrichtlinie geben die Nutzer Facebook im Grunde eine Generalvollmacht, alle sie betreffenden personenbezogenen Daten zu sammeln.

Umso wichtiger ist es, dass Bibliotheken, Schulen, Hochschulen und andere Einrichtungen den Bürgerinnen und Bürgern ausreichend Gelegenheit bieten, Privatheitskompetenz zu erwerben. Studien belegen, dass Jugendliche und junge Erwachsene nur über eine geringe Privatheitskompetenz in Online-Umgebungen verfügen.[11] Gleichzeitig ist jedoch zu beobachten, dass Nutzer mit höherer Privatheitskompetenz keineswegs ein signifikant anderes Verhalten im Hinblick auf den Schutz ihrer personenbezogenen Daten zeigen. Auch wenn dem Schutz der Privatsphäre hohe Priorität zugeschrieben wird, verzichten diese Nutzer nur in sehr begrenztem Umfang auf Angebote, welche die Preisgabe personenbezogener Daten verlangen. Selbst bei vorhandenem Problembewusstsein werden nur selten technische Maßnahmen ergriffen, um den Zugriff auf die eigenen personenbezogenen Daten einzuschränken.[12] In der Forschung wird diese Diskrepanz zwischen Einstellung und Verhalten als Privacy-Paradox bezeichnet.[13] Es gibt dafür verschiedene Erklärungsansätze.[14] Zum einen wird geltend gemacht, dass die negativen Folgen der Verletzung von Privatheit nicht unmittelbar zu spüren sind und daher unterschätzt werden. Ein anderes Erklärungsmodell hält Resignation für den wahren Grund. Demnach lehnt die große Mehrheit die ungewollte Preisgabe personenbezogener Daten ab, sieht dies jedoch als unvermeidlich an, da jeder Versuch, sich dagegen zu wehren aufgrund der Marktmacht der Betreiber Sozialer Netzwerke zum Scheitern verurteilt sei. Diese These steht in krassem Widerspruch zu der von den Betreibern aufgestellten Behauptung, ihr Geschäftsmodell beruhe auf einer allgemein akzeptierten Tauschbeziehung.[15]

10 Facebook 2016.
11 Vgl. Masur / Teutsch / Dienlin / Trepte 2017: 183.
12 Vgl. Masur / Teutsch / Dienlin / Trepte 2017: 183.
13 Vgl. Funiok 2016: 78.
14 Vgl. dazu Wehofsits 2016: 28f.
15 Vgl. Wehofsits 2016: 29.

3. Verschleierung der Grenze zwischen öffentlicher und privater Sphäre

Aus Sicht der Nutzer wird der Kommunikationsmodus in Sozialen Netzwerken in der überwiegenden Zahl der Fälle als Konversation wahrgenommen und nicht als Publikation.[16] Die Nutzer glauben, ausschließlich im und für das individuelle Freundschaftsnetzwerk zu kommunizieren. Denn dieses Netzwerk ist dadurch zustande gekommen, dass die Betroffenen in jedem Fall über die Aufnahme selbst entschieden haben. In den meisten Fällen aber ging den Freundschaftsanfragen ein Vorschlag der Betreiber der Sozialen Netzwerke voraus. Diese Vorschläge werden gewonnen durch einen automatisierten Abgleich der Persönlichkeitsprofile. Auf diese Weise kommen dann auch solche Personen für die Aufnahme in das eigene Freundschaftsnetzwerk in Betracht, mit denen lediglich der Besuch derselben Schule verbindet oder die mit mehreren Mitgliedern des eigenen Netzwerkes befreundet sind. Trotz der Tatsache, dass auf diese Weise nicht selten auch eher fernstehende Personen in das individuelle Netzwerk aufgenommen werden, dominiert im individuellen Bewusstsein der Eindruck, sich tatsächlich unter Freunden zu befinden. So entsteht eine soziale Vertrautheit, die der face-to-face-Kommunikation entspricht, während vergessen wird, dass im Hintergrund Dritte anwesend sind: die Netzbetreiber, die werbende Industrie sowie Polizei und Geheimdienste.[17] Deren Interessen bestehen in der erfolgreichen Platzierung personalisierter Werbung, im Weiterverkauf der Persönlichkeitsprofile zu Werbezwecken und in umfassender Überwachung.

Online-Kommunikation in Sozialen Netzwerken ist nie rein privat, sondern immer latent öffentlich.[18] In dieser Kombination aus öffentlicher Privatheit oder privater Öffentlichkeit verschwimmt die Grenze zwischen öffentlicher und privater Sphäre. Diese Grenze aber ist demokratischen Gesellschaften strukturell eingeschrieben und für ihr Funktionieren elementar, damit sich eine kritische Öffentlichkeit herausbilden kann. Es läge in der gesellschaftlichen Verantwortung der Betreiber

16 Vgl. Bieber 2016: 70.
17 Vgl. Funiok 2016: 78.
18 Vgl. Bieber 2016:78.

Sozialer Netzwerke, ihre Nutzer, die in Wahrheit Kunden sind, auf die tatsächlichen Strukturen und Sachverhalte gezielt hinzuweisen, damit ihnen bewusst wird, dass Kommunikation in Sozialen Netzwerken eben keine private Kommunikation mehr ist, sondern einen von ihnen nicht kontrollierbaren Adressatenkreis erreicht.

De facto jedoch animieren die Betreiber Sozialer Netzwerke ihre Nutzer zur Veröffentlichung des Privaten, zur unbewussten Selbstentäußerung in einem verdeckten, von ökonomischen Verwertungsinteressen und politischen Kontrollansprüchen geprägten Umfeld.[19] Genutzt werden die personenbezogenen Daten dann von Algorithmen, die auf diese Interessen zugeschnitten sind, um über Empfehlungen und personalisierte Werbung zum Konsum zu animieren. Soziale Netzwerke setzen damit in digitalen Kontexten fort, wie Kritiker hervorheben, was Jürgen Habermas schon 1981 als „Kolonialsierung der Lebenswelt" bezeichnet hat.[20] Zudem sehen sie in der durchgängigen Inklusion der Datenspuren auch intimer Ereignisse in das Trackingsystem eine Bestätigung des von Gilles Deleuze konstatierten Übergangs von der Disziplinargesellschaft in die Überwachungsgesellschaft.[21] *Während die Überwachung in analogen Disziplinargesellschaften in Institutionen und abgrenzbaren Bereichen wie Fabriken, Krankenhäusern oder Schulen erfolgt, ist die digitale Überwachung penetrant und ubiquitär: eine Grenze zwischen privat und öffentlich existiert nicht mehr.*[22]

4. Hassreden, Desinformation und Fake News

Der subjektive Eindruck, in einer quasi privaten Umgebung zu kommunizieren sowie die Möglichkeit, die Autorschaft zu anonymisieren oder hinter einem Pseudonym zu verbergen, erhöht die Gefahr, dass Kommunikationsfreiheit umschlägt in Enthemmung.[23] Verstärkt wird dieser Effekt durch die Unmittelbarkeit vieler Reaktionen. Die Kommentare werden häufig abgeschickt, kurz nachdem deren Gegenstand

19 Vgl. Simanowski 2016: 72
20 Vgl. Habermas 1988: 522.
21 Vgl. Deleuze 1993.
22 Vgl. Figueiredo / Bolaño 2017: 36.
23 Vgl. Heesen 2016c: 55.

zur Kenntnis genommen worden ist und bevor eine nüchternere und reflektiertere Haltung eingenommen werden konnte. Auch aus diesem Grund kommt es in Sozialen Netzwerken häufiger zu hochgradig emotional aufgeladenen Stellungnahmen, zu übler Nachrede und zu persönlichen Verunglimpfungen. Verstärkt wird aber auch der Trend zu radikalen Äußerungen, mit denen nicht nur die Grenzen des guten Geschmacks übertreten werden, sondern die darüber hinaus Forderungen enthalten, die weder ethisch noch rechtlich hinnehmbar sind. Dabei handelt es sich um sog. Hassreden, zu denen u.a. rassistische und ausländerfeindliche Hetze, menschenverachtende Herabwürdigungen, sexistische Beleidigungen oder unverhohlene Aufrufe zu Straf- und Gewalttaten gehören. Besonders häufig finden sich Aussagen vergleichbaren Inhalts in geschlossenen Gruppen etwa bei Facebook. Manche Teilnehmer lassen ihrem blanken Hass, ihren Gewaltphantasien und ihren xenophoben Projektionen freien Lauf.

Von den Hassreden zu unterscheiden, sind gezielte Desinformationskampagnen. Dabei können beide Phänomene durchaus inhaltlich identische Aussagen enthalten. Der Unterschied besteht in der Wirkungsabsicht der Sender. Während Hassreden eher von Einzelpersonen ausgehen und Einzelmeinungen artikulieren, handelt es sich bei Desinformation meist um Aktivitäten, für die Interessengruppen verantwortlich sind und die darauf zielen, Verwirrung zu stiften und die öffentliche Meinung in propagandistischer Absicht zu manipulieren. Für Desinformation, die über Soziale Netzwerke verbreitet wird, hat sich in jüngster Zeit der Begriff *Fake News* eingebürgert. Es handelt sich dabei um Falschmeldungen, die über soziale Netzwerke in manipulativer Absicht verbreitet werden und die sich meist gleichzeitig als vertrauenswürdige Quelle ausgeben.[24] Fake News richten sich an die Gefühle der Adressaten, um Stimmungen zu schüren und die daraus resultierende Aufregung in den Dienst der eigenen, meist politischen Ziele zu stellen.

Ein wichtiges Instrument zur Verbreitung von Fake News sind Social Bots. Dahinter verbergen sich Computerprogramme, die automatisiert auf vorher festgelegte Impulse reagieren. So ist es z.B. möglich, einen Social Bot bei Twitter zu installieren, der mit falschem Namen, Profilbild, Posts und Followern versehen wird und für andere als Account einer

24 Vgl. Sinders 2017: 59.

natürlichen Person erscheint. Social Bots reagieren dann mittels computerlinguistischer Verfahren auf bestimmte Hashtags und versenden („retweeten") dann vorgefertigte Antworten. In ähnlicher Weise werden Social Bots in großer Zahl auch auf Facebook eingesetzt, um Falschinformationen zu „liken". Dies sorgt für Amplifikationseffekte durch simulierte Zustimmung, in deren Folge die Popularität der entsprechenden Aussagen für die Algorithmen steigt. Damit erhalten die entsprechenden Inhalten erhöhte Sichtbarkeit, stärkere Verbreitung und möglicherweise größerer Akzeptanz. Über Social Bots lassen sich Fake News in Echtzeit verbreiten und Minderheitsmeinungen massiv verstärken.[25] Eine weitere Möglichkeit zur Verbreitung von Fake News in Sozialen Netzwerken besteht in sog. Troll-Farmen, Troll-Fabriken oder Troll-Armeen. In diesen Fällen sind es Menschen, die dafür bezahlt werden, mittels fingierter Accounts in Sozialen Netzwerken Falschinformationen in propagandistischer Absicht zu verbreiten.[26]

Maßnahmen gegen Fake News in Sozialen Netzwerken zu ergreifen, ist aus ethischer Sicht nicht nur unbedenklich sondern in vielen Fällen auch geboten. Voraussetzung dafür ist allerdings, dass es klare Kriterien zur eindeutigen Identifikation gibt und die Abwehrmaßnahmen in gleicher Weise erfolgen, unabhängig von Inhalten, Urhebern und Adressaten. Anders verhält es sich bei Hassreden. Die Schwierigkeit in diesem Fall besteht darin, die Grenze zwischen Hassrede und Meinungsfreiheit eindeutig zu ziehen. In ihrem Selbstverständnis verstehen sich Soziale Netzwerke nicht als Content Provider, sondern als technikbasierte Distributionsplattform.[27] Daher lehnen sie eine Haftung für die Inhalte grundsätzlich ab.[28] Mit dem Netzdurchsetzungsgesetz sind die Betreiber Sozialer Netzwerke in Deutschland seit Ende 2017 verpflichtet, alle Dokumente, die ihnen gemeldet werden, weil sie möglicherweise Hassreden enthalten, zu überprüfen und gegebenenfalls zu löschen. Dem kommen Facebook, Twitter, YouTube und andere offenbar mittlerweile

25 Vgl. Neudert 2017: 2; vgl. auch Sowa 2017: 62-66.
26 Vgl. Schwarz 2017.
27 Vgl. Veddern 2017: 130.
28 In den Nutzungsbedingungen heißt es explizit: „Wir sind nicht verantwortlich für beleidigende, unangemessene, obszöne, rechtswidrige oder auf sonstige Art anstößige Inhalte oder Informationen, denen du eventuell auf Facebook begegnest. Wir sind nicht für das Verhalten von Facebook-NutzerInnen verantwortlich, weder online noch offline." Facebook 2015.

auch nach. Kritik entzündet sich zum einen daran, dass die Löschpraxis weitgehend intransparent bleibt. Zum anderen wird moniert, dass der Staat damit hoheitliche Aufgaben an Privatunternehmen delegiert. Unabhängig vom Netzdurchsetzungsgesetz hat Facebook aber schon in der Vergangenheit Beiträge gelöscht, die gegen „Gemeinschaftsstandards" verstoßen haben. Diese Standards orientieren sich offenbar an der Werteordnung der USA, des Landes, in dem das Unternehmen seinen Sitz hat. Entfernt wurden z.T. Bilder und Texte, die in Europa eher als harmlos angesehen werden.

Aus ethischer Sicht ist zu fordern, dass Löschungen nach einem transparenten Kriterienkatalog erfolgen. Betroffene müssen unverzüglich darüber informiert werden, wenn von ihnen hochgeladene Inhalte gelöscht worden sind. Jede Löschung ist detailliert unter Bezugnahme auf den Kriterienkatalog zu begründen. Die bislang gängige Praxis, entweder gar keine Begründung zu geben oder pauschal zu behaupten, es habe ein „Verstoß gegen Gemeinschaftsstandards" vorgelegen, ist inakzeptabel. Ferner müssen Betroffene die Möglichkeit haben, vor einer zweiten Prüfungsinstanz Einspruch einzulegen. Wichtig ist darüber hinaus, dass die Freiheit der Kunst und der Satire nicht durch rigides Löschen eingeschränkt wird.

5. Zusammenfassung und Forderungen

Die Auseinandersetzung mit Sozialen Netzwerken unter ethischen Gesichtspunkten hat nicht zum Ziel, deren Funktionalität und Gebrauchswert grundsätzlich in Abrede zu stellen. Stattdessen geht es darum, auf ethisch problematische Aspekte aufmerksam zu machen, einen Anstoß zu deren Beseitigung zu geben und Missbrauch grundsätzlich zu erschweren. Es zeigt sich, dass Soziale Netzwerke aufgrund ihres Geschäftsmodells personenbezogene Daten in größtmöglichem Umfang kumulieren, um daraus Persönlichkeitsprofile zu entwickeln, die vor allem zu Werbezwecken eingesetzt werden. Nutzern bleibt dieser Zusammenhang und vor allem das Ausmaß der Datenauswertung oft verborgen. Selbst wenn diese Zusammenhänge bekannt sind, führt die marktbeherrschende Stellung etwa von Facebook dazu, dass gravie-

rende Nachteile in Kauf genommen werden. Zu fordern ist, dass die Geschäftspraktiken transparent gemacht werden, Nutzer Zugriff auf die über sie gespeicherten Daten erhalten und gestufte Opt-out-Funktionen angeboten werden. Die Betreiber leisten der Illusion Vorschub, die Kommunikation in Sozialen Netzwerken sei vorwiegend privater Natur. Der Gesetzgeber sollte dafür sorgen, dass die Nutzer erfahren, wer Zugriff auf ihre Daten hat und damit verstehen, dass alle in Sozialen Netzwerken vollzogenen Aktionen latent öffentlich sind. Schließlich bieten Soziale Netzwerke ein ideales Umfeld für Hassreden, Desinformation und Fake News. Gegenmaßnahmen der Betreiber müssen auf der Grundlage eines transparenten und detaillierten Kriterienkatalogs erfolgen und detailliert begründet werden. Davon Betroffene müssen informiert werden und die Möglichkeit zum Widerspruch erhalten.

Grundsätzlich ist es Aufgabe der staatlichen Daseinsvorsorge, allen Bürgerinnen und Bürgern in der Informationsgesellschaft die Chance zu geben, in ausreichendem Maße Informationskompetenz zu erwerben, um die Funktionsweise sowie die Vor- und Nachteile Sozialer Netzwerke angemessen einschätzen zu können. Geeignet dafür sind vor allem Bibliotheken, die diese Kompetenzen in Kooperation mit Schulen, Hochschulen und Einrichtungen der Erwachsenenbildung systematisch vermitteln sollten. Zu fordern ist ferner, dass Behörden, Institutionen, Unternehmen, Vereine und Verbände, die gegenwärtig arglos dazu auffordern, ihnen z.B. auf Facebook zu folgen, immer auch darauf hinweisen, welche Vorsichtsmaßregeln beachtet werden sollten und Kontakte zu solchen Stellen nennen, die über den vertretbaren Umgang mit und angemessenes Verhalten in Sozialen Netzwerken aufklären. Ziel eines anhaltenden öffentlichen Diskurses sollte es sein, Klarheit darüber zu gewinnen, durch welche Maßnahmen Politik und Gesellschaft verhindern können, dass über Soziale Netzwerke öffentliche Meinungsbildung manipuliert wird.

Quellen

BIEBER, Christoph (2016): Öffentlichkeit. In: Heesen, Jessica (Hrsg.): Handbuch Medien- und Informationsethik. Stuttgart: Metzler, 67–73.

CONRAD, Conrad (2016): Neue Perspektiven und Gefahren der Gesichtserkennung. In: Datenschutz Notizen. 27.6.2016. https://www.datenschutz-notizen.de/neue-perspektiven-und-gefahren-der-gesichtserkennung-1915015/ (5.2.2017).

DELEUZE, Gilles (1993): Postskriptum zu den Kontrollgesellschaften. In: Ders.: Unterhandlungen 1972–1990. Frankfurt a.M.: Suhrkamp, 254–262.

FACEBOOK 2015: Nutzungsbedingungen. 30.Januar.2015. https://www.facebook.com/legal/terms (9.2.2018).

FACEBOOK (2016): Datenrichtlinie 29. September 2016. https://www.facebook.com/policy.php (8.2.2018).

Facebook darf Daten über Nichtmitglieder sammeln (2016). In: Spiegel online. 30.6.2016. http://www.spiegel.de/netzwelt/netzpolitik/facebook-darf-daten-ueber-nicht-mitglieder-sammeln-a-1100604.html (2.2.2018).

FIGUEIREDO, Carlos, BOLAÑO, César (2017): Social Media and Algorithms. Configurations of the Lifeworld Colonization by New Media. In: International Review of Information Ethics. 26, 2017, 12, S. 26-38. http://www.i-r-i-e.net/inhalt/026/IRIE-26-Marx-12-2017-4.pdf (9.2.2018).

FUNIOK, RÜDIGER (2016): VERANTWORTUNG. IN: HEESEN, JESSICA (HRSG.): Handbuch Medien- und Informationsethik. Stuttgart: Metzler, 74–80.

HABERMAS, Jürgen (1988): Theorie des kommunikativen Handelns. 2. Bd. Zur Kritik der funktionalistischen Vernunft. Frankfurt a.M.: Suhrkamp.

HEESEN, Jessica (2016): Freiheit. In: Heesen, Jessica (Hrsg.): Handbuch Medien- und Informationsethik. Stuttgart: Metzler, 52–58.

MASUR, Philipp K., Doris TEUTSCH, Tobias DIENLIN, Sabine TREPTE (2017): Online-Privatheitskompetenz und deren Bedeutung für demokratische Gesellschaften. In: Forschungsjournal Soziale Bewegungen. 30, 2, 180–189.

NEUDERT, Lisa-Maria (2017): Angriff der Algorithmen. Wahlmanipulation im Internet? Veranstaltung. „(Des)Information?! Politische Meinungs- & Willensbildung in sozialen Netzwerken". Friedrich-Ebert-Stiftung. *Köln am 08. Juni 2017.* https://www.fes.de/index.php?eID=dumpFile&t=f&f=15002&token=b0e0303aa9e08744190db33cbc6bb90ec53ed5c6 (9.2.2018).

REUTER, Markus (2017): Facebook weitet Gesichtserkennung aus. In: Netzpolitik.org 21.12.2017. https://netzpolitik.org/2017/facebook-weitet-gesichtserkennung-aus/ (5.2.2018)

SCHWARZ, Karolin (2017): Trolle, Influencer, Evangelisten. Heinrich-Böll-Stiftung. 9.2.2017. https://www.boell.de/de/2017/02/09/trolle-influencer-evangelisten (8.2.2018).

SIMANOWSKI, Roberto (2016): Facebook-Gesellschaft. Berlin: Mathes u. Seitz.

SINDERS, Caroline (2017): Ethische Systementwicklung im Zeitalter emotionaler Schadsoftware. Fake News, maschinelles Lernen und die Erzeugung von Transparenz in einer Zeit des Misstrauens in großen Netzwerken. In: Otto, Philipp, Eike Gräf (Hrsg.): 3TH1CS. Die Ethik der digitalen Zeit. Berlin: iRights.media, 56–64.

SOWA, Alexandra (2017): Digital Politics. So verändert das Netz die Demokratie. 10 Wege aus der digitalen Unmündigkeit. Bonn: J.H.W. Dietz.

STATCOUNTER (2018). Social Media Stats worldwide Dec 2016 – Jan 2018. Statcounter. http://gs.statcounter.com/social-media-stats (2.2.2018).

USAGE OF SOCIAL WIDGETS FOR WEBSITES (2018). In: W3Techs 2.2.2018. http://www.spiegel.de/netzwelt/netzpolitik/facebook-darf-daten-ueber-nicht-mitglieder-sammeln-a-1100604.html (2.2.2018).

VEDDERN, Michael (2017): Hate Speech, Fake News auf Facebook, Twitter & Co. In: Huse, Ulrich Ernst (Hrsg.): Zensur und Medienkontrolle in demokratischen Gesellschaften. Wiesbaden: Harrassowitz, 127–141. (= Kodex. 7, 2017)

Was Facebook mit ihren WhatsApp-Daten macht (2017). In: Spiegel online. 18.5.2017. http://www.spiegel.de/netzwelt/apps/was-facebook-mit-ihren-whatsapp-daten-macht-a-1148318.html (5.2.2018).

WEHOFSITS, Anna (2016): Big Data. Ethische Fragen. Hrsg. Vodafone Institut für Gesellschaft und Kommunikation. Oktober 2016. http://www.vodafone-institut.de/wp-content/uploads/2016/10/Big-Data_Ethische-Fragen.pdf (20.2.2018).