

März 2019 · Alexander Sänglerlaub

Der blinde Fleck digitaler Öffentlich- keiten

Warum sich Desinformationskam-
pagnen in sozialen Netzwerken
kaum systematisch analysieren
lassen



Think Tank für die Gesellschaft im technologischen Wandel

Executive Summary

Auch bei der EU-Parlamentswahl im Mai besteht Sorge vor Desinformationskampagnen, die online stattfinden und so Einfluss auf den Wahlprozess nehmen konnen. Derzeit ist es fast unmoglich, systematische Untersuchungen uber die Verbreitungswege, die beteiligten Akteure und die Reichweite von Desinformationskampagnen innerhalb der Social-Media-Plattformen anzustellen. Wir konnen derzeit kaum systematisch untersuchen, wie viel Desinformation sich auf welchen Social-Media-Plattformen befinden, wie sehr das Design der Plattformen zur Verbreitung von Falschinformationen beitragt, wer Desinformation systematisch verbreitet oder wie stark der Einfluss auf unsere politischen Debatten ist. Dies ist nicht nur ein Problem fur Fact-Checking-Organisationen oder Behorden, die versuchen, gegen Hetze oder Propaganda vorzugehen. Es ist auch ein enormes Problem fur politische Entscheidungstrager:innen, die derzeit in vielen Landern aber auch supranational, versuchen, wirksame Manahmen zum Schutz demokratischer digitaler offentlichkeiten zu entwickeln.

Der Zugriff auf die dafur benotigten Daten von Facebook, Twitter, YouTube, Instagram und anderen Plattformen ist derzeit stark eingeschrankt, sodass Untersuchungen der digitalen offentlichkeit quasi blind sind. Die benotigten Daten werden von den Plattformen zwar erhoben, sie stehen der offentlichkeit aber nicht zur Verfugung. Dabei geht es explizit nicht um die privaten Daten von Nutzer:innen, sondern um die Daten von Beitragen, die in sozialen Medien offentlich geteilt werden – etwa von Firmen, Nachrichtenseiten, Politiker:innen oder Influencer:innen.

Fur die systematische Analyse solcher offentlichen Beitrage sind unterschiedliche Datenpunkte relevant. Dazu gehoren unter anderem technische Daten (wer hat den Beitrag wann erstellt), Reichweitendaten (wie vielen Nutzer:innen wurde der Beitrag angezeigt, wie viele Accounts haben mit dem Beitrag interagiert, indem er geliket oder geteilt wurde), Suchergebnisdaten (uber welche Stichworter kann man den Beitrag in Suchmaschinen oder auf der Plattform selbst finden), Daten daruber, ob der Beitrag als Werbeanzeige geschaltet wurde und wie viel Geld dafur ausgegeben wurde sowie Angaben dazu, ob der Beitrag nachtraglich geandert wurde.

Alle diese Daten konnen derzeit nicht systematisch eingesehen werden. Dies gilt fur Facebook, Twitter, Instagram und YouTube, die in Bezug auf Nutzer:innenzahlen zu den groten sozialen Netzwerken in Deutschland zahlen und die damit auch relevant fur die offentliche Meinungsbildung sind. Sie alle



Alexander Sangerlaub

Marz 2019

Der blinde Fleck digitaler offentlichkeiten

stellen nur sehr vereinzelt Schnittstellen bereit, die aber keine umfassenden systematischen Analysen ermoglichen.

Wie problematisch es ist, wenn Daten daruber fehlen, welche Social-Media-Desinformationskampagnen kursieren, wie sie sich verbreiten und welche Akteure an ihrer Verbreitung beteiligt sind, zeigten die Vorfalle in Chemnitz im Sommer 2018, bei denen ein junger Mann getotet wurde. In der Folge gab es Ausschreitungen durch Rechtsextreme, die sich auch online organisiert und durch Desinformation Stimmung gemacht haben. Versucht man, diese Desinformationskampagnen systematisch zu analysieren, stot man je nach Art des Beitrags schnell an die Grenzen. Reine Textbeitrage konnen auf manchen Plattformen zumeist noch durch die Suchfunktion gefunden werden, etwa uber das Stichwort "Chemnitz". Inhalte in Bild- und Videodaten lassen sich aber so nicht finden, obwohl es durch automatische Texterkennung technisch moglich ware. Doch auch die Suchfunktion selbst ist problematisch: Die Reihenfolge, in der Ergebnisse angezeigt werden, birgt das Potential, zur Verbreitung von Desinformation beizutragen. Ob ein Beitrag bestimmten Nutzer:innen als Werbung angezeigt wird, um die Sichtbarkeit zu erhohen, ist auf Facebook derzeit nicht systematisch nachvollziehbar.

Der Zugang zu relevanten offentlichen Daten der Social-Media-Plattformen muss verbessert werden, damit Forschung und Politik in Sachen Desinformation nicht langer im Dunkeln tappen. Die wenigen Datenschnittstellen, die etwa Google oder Facebook auf freiwilliger Basis fur politische Werbung im Vorfeld von Wahlen anbieten, reichen nicht aus. Benotigt werden Datenzugange, die sowohl das Echtzeit-Monitoring von sozialen Netzwerken ermoglichen, als auch den Zugriff auf Daten aus der Vergangenheit. Erst wenn diese Daten vorliegen, konnen Regierungen und Behorden wirksame Manahmen gegen Desinformation entwickeln und uberprufen. Gleichzeitig wurde dies auch die Wissenschaft in die Lage versetzen, fundierte Studien zu den Herausforderungen unserer digitalen offentlichkeit zu erstellen.

Inhalt

1. Blinde Flecken, viele Fragen

Die Demokratisierung unserer Öffentlichkeit, an der jede und jeder heute mehr denn je teilhaben kann, ist ein großer Gewinn der demokratischen Öffentlichkeiten des 21. Jahrhundert. Doch es gibt eine Kehrseite: Populismus, Hate Speech, Propaganda, Desinformation im Netz sind ebenso zu einem festen Bestandteil digitaler Öffentlichkeit geworden. Politik, Regulierungsbehörden, Fact-Checking-Organisationen und viele zivilgesellschaftliche Organisationen haben reagiert und versuchen derzeit mit verschiedenen Mitteln, digitale Desinformation zu bekämpfen. Doch um solche Initiativen sinnvoll und zielgerichtet umsetzen und evaluieren zu können, ist es unabdingbar, belastbare Informationen über das Ausmaß, Ausprägungen und Akteuren von Desinformationskampagnen zu erlangen: Wie viel und welche Formen von Desinformation befinden sich auf den Social-Media-Plattformen? Welche außer- und innerstaatlichen Akteure versuchen mit welchen Methoden Einfluss auf Debatten zu nehmen? Wie sehr trägt das Design der Plattformen zur Verbreitung von Falschinformationen bei? Wie erfolgreich ist das Fact-Checking? Wer kreiert Desinformation, wer teilt sie, welche Rolle spielt der klassische Journalismus und was bedeutet das alles für die Güte unserer Debatten in der Demokratie?

Das sind relevante Fragen, auf die derzeit nur schwer Antworten zu finden sind. Denn derzeit ist es für Politik, Wissenschaft, Journalismus (darunter auch die Fact-Checking-Organisationen), NGOs weitestgehend unmöglich, solche Fragen umfassend zu beantworten. Was innerhalb sozialer Netzwerke passiert, entzieht sich derzeit an vielen Stellen einer systematischen Analyse. Es fehlen schlichtweg die Zugänge zu wichtigen, öffentlichen Daten. Ohne solche Daten können höchstens – falls überhaupt – stichprobenartige Eindrücke darüber gewonnen werden, was innerhalb digitaler Öffentlichkeit sozialer Netzwerke kursiert.

Wie sich dieser Blindflug auf die mediale und politische Öffentlichkeit auswirkt, kann man anhand der Vorgänge im August 2018 in Chemnitz gut erkennen. Hier hat die politische Öffentlichkeit inzwischen durch aufwendige Recherchen von Fact-Checking-Organisationen und Journalist:innen zumindest eine ungefähre Ahnung davon, wie hier die Plattformen als Transmitter und Katalysatoren zur Verbreitung von Desinformation beigetragen haben. Gerüchte, Lügen und falsche Tatsachen zu den Tathergängen verbreiteten sich über YouTube, Facebook und Twitter wie Lauffeuer und hatten ihren Anteil an der starken Mobilisierung rechtsextremer Kräfte auf den Straßen von Chemnitz. Diesen Einzelfall möchten wir nutzen, um zu zeigen, welche Daten

es eigentlich brauchte, um Desinformationskampagnen systematisch zu beobachten. Denn demokratische politische offentlichkeiten sind nur funktionsstuchtig, wenn alle teilnehmenden Akteure auch beobachten konnen, was in diesen offentlichkeiten passiert, solange sie eine relevante Rolle fur unsere digitalen offentlichkeiten in der Mediennutzung spielen.¹

Insbesondere Facebook hat sich dabei in den letzten Jahren unter dem Druck der offentlichkeit nicht etwa weiter geoffnet und Zugriffe auf ihren hohen Datenschatz zur digitalen offentlichkeit ermoglicht. Im Gegenteil wurden nach dem Skandal um Cambridge Analytica Datenschnittstellen geschlossen, sodass die Beobachtung nun noch schlechter moglich ist, als sie es ohnehin schon war.² Dass durch Cambridge Analytica private Daten von Nutzer:innen illegal weiterverbreitet wurden, sollte generell nicht als Vorwand fur Social-Media-Unternehmen fungieren, offentliche Daten unter Verschluss zu halten. Dazu gehoren eben nicht die personlichen Informationen wie Privatnachrichten oder sensible personenbezogene Daten, sondern Postings die als Werbeanzeigen geschaltet werden, auf YouTube als Video hochgeladen, in Bildform uber Facebook, Twitter oder Instagram als Meme geshared und geliked oder sogar von Medien aufgenommen und weiterverbreitet werden, weil diese die Herkunft bestimmter Information zuweilen nur ungenau prufen.³

Damit losen soziale Netzwerke eine tiefgehende Disruption auf unsere offentlichkeiten aus. Propaganda, Falsch- und Desinformation konnen sich ungehindert verbreiten⁴ und es gibt kaum Moglichkeiten, dieses Phanomen unabhangig und datenbasiert zu untersuchen.

Dieses Papier zeigt am Beispiel der Vorfalle in Chemnitz, was fur offentliche Daten derzeit fur die Bekampfung von Desinformation – das heit fur wissenschaftliche Forschung, Fact-Checking-Organisationen und Journalist:innen fehlen und welche Probleme dies fur Politik und Gesellschaft erzeugt. Es geht, auch das soll deutlich werden, dabei nicht um die privaten oder perso-

1 Reuters Institute (2018): Digital News Report 2018. <http://media.digitalnewsreport.org/wp-content/uploads/2018/06/digital-news-report-2018.pdf?x89475>

2 Axel Bruns (25.04.2018): Facebook Shuts the Gate after the Horse Has Bolted, and Hurts Real Research in the Process. <https://medium.com/@Snurb/facebook-research-data-18662cf2cacb>

3 Alexander Sangerlaub/Miriam Meier/Wolf Dieter-Ruhl (2018): Fakten statt Fakes. Verursacher, Verbreitungswege und Wirkungen von Fake News im Bundestagswahlkampf 2017, <https://www.stiftung-nv.de/de/publikation/fakten-statt-fakes-verursacher-verbreitungswege-und-wirkungen-von-fake-news-im>

4 Soroush Vosoughi, Deb Roy, Sinan Aral (2018): The spread of true and false news online. In Science: 03/2018, Vol. 359, <http://science.sciencemag.org/content/359/6380/1146.full>

nenbezogene Daten der Nutzer:innen, sondern nur um Daten, die eigentlich ohnehin offentlich sind oder es sein sollten.

Daruber hinaus pladiert das Papier dafur, einen kontrollierten Datenzugang fur zu schaffen, damit Zivilgesellschaft, Wissenschaft und Gesetzgeber eine Moglichkeit erhalten, die Probleme in den Plattformen besser zu verstehen und offentlich nachzeichnen konnen.

Im letzten Kapitel werden neue und bisherige Ansatze, auch der Plattformen, vorgestellt, um zu zeigen, wie der Zugang konkret in der Anwendung aussehen kann.⁵ Es ist dringend Zeit, die zahllosen offentlichen Daten, die Plattformen wie Facebook ohnehin erheben, der Gesellschaft einfach zuganglich zu machen, damit wir die Vorgange in den Plattformen besser verstehen.

2. Daten, Datenschnittstellen und offentlich vs. privat

Viele Daten in den sozialen Netzwerken sind offentlich einsehbar –weil sie per Definition offentlich sind: seien es Tweets bei Twitter, Beitrage von Spiegel Online bei Facebook oder Videos von alternativen Medienanbietern, wie RT Deutsch, bei YouTube. Uber die Suchfunktionen der Plattformen, wie Twitter, Instagram, Facebook oder YouTube, genauso uber Suchmaschinen, wie Google, lassen sich diese Inhalte auffinden. Doch nur weil sich Inhalte auffinden lassen, sind sie noch lange nicht systematisch fur die Wissenschaft oder Fact-Checking-Organisationen analysierbar. Hierfur bedarf es Daten-

⁵ Eine Moglichkeit ware hier ein ahnliches Transparenzangebot zu machen, wie mit dem Wahlwerberegister. Diese wurden von Facebook und Google zur Europawahl angekundigt, sind aber bisher noch nicht veroffentlicht worden.

Wahlwerberegister. Facebook nennt dieses Tool „werbebibliothek“, diese ist (Stand: 08.03.2019) bisher fur die USA, Grobritannien, Indien und Brasilien verfugbar: https://www.facebook.com/ads/archive/?active_status=all&ad_type=political_and_issue_ads&country=ALL, Google nennt seine ubersicht „Politische Werbung bei Google“, diese enthalt bisher (Stand 08.03.2019) nur die USA: <https://transparencyreport.google.com/political-ads/overview>

schnittstellen⁶, die Daten beispielsweise fur Social Media Intelligence Tools⁷ zuganglich machen. Diese Tools ermoglichen es, die Daten aufzubereiten, auszuwerten, graphisch darzustellen, aggregierbar oder kategorisierbar zu machen. Auch gibt es Daten, die fur die offentlichkeit zwar relevant waren, aber bisher nicht sichtbar sind, weil die Plattformen sie zwar erheben, aber unter Verschluss halten. Dazu gehoren beispielsweise Daten zum Erfolg des Fact-Checkings als Manahme gegen Desinformation.

Die verschiedenen Typen von Daten wollen wir in diesem Kapitel vorstellen, um deutlich zu machen, welche Daten fur die politische offentlichkeit von den Plattformen zuganglich gemacht werden sollten. Das anschließende Kapitel zur „Klaviatur der Desinformation“ im konkreten Anwendungsfall zu Chemnitz soll noch einmal die Dringlichkeit der Zuganglichkeit dieser Daten unterstreichen sowie das vielleicht etwas abstraktere Kap. 2 durch Beispiele unterfuttern.

Welche Daten sind relevant und offentlich?

Soziale Netzwerke erheben eine Vielzahl von nutzerspezifischen Verhaltensdaten, die Aufschluss uber die politische Einstellung, die sexuelle Orientierung oder anderweitig grundprivate Daten einzelner Personen geben. All

⁶ **Datenschnittstellen**, bzw. „Anwenderprogrammierschnittstellen“ (englisch API fur application programming interface) ermoglichen die Anbindung von einer Software an die andere. Der Zugriff auf die Datenschnittstellen ermoglicht es wissenschaftlicher Forschung, Daten einfach zu erheben, um diese dann auszuwerten. **Social Media Intelligence-Tools** nutzen diese Anbindung, um auch ihr grafisches Interface mit den Plattformdaten zu verbinden, sodass die Anwendung und Analyse der Daten auch ohne Programmierkenntnisse moglich sind. Auch haben die Schnittstellen rechtlich Bedeutung, da eine offentlich verfügbare oder eingekaufte Anbindung an eine Schnittstelle das Arbeiten mit den zur Verfugung gestellten Daten erlaubt – anders als beim Scrapen (also dem illegalen Abschöpfen von Daten von auen, das durch die meisten Terms of Service der Plattformen untersagt ist). Die Plattformen wiederum haben den Vorteil, dass sie innerhalb der Schnittstellen bestimmen konnen, welche Daten sie freigeben und damit eine bessere ubersicht uber das eigene Datenmanagement haben.

⁷ Am Markt gibt es zahlreiche ahnliche Tools zu dem von uns 2017 benutzten Tool Talkwalker wie BuzzSumo, Pulsar, Meltwalter, Crimson Hexagon, complexium, Alto und andere. Sie bieten alle auch **Social Media Intelligence** an, also die systematische Analyse von Daten aus sozialen Netzwerken. Nicht immer sind diese – wie bei Talkwalker – gepaart mit Daten aus klassischen Medienangeboten. All diese Tools sind allerdings in ihrer Funktionstuchtigkeit auch davon abhangig, welche Schnittstellen die jeweiligen Plattformen (wie Facebook, Twitter, etc.) fur den Datenzugriff gewahren. Fast alle Tools unterliegen kommerziellen Interessen, ahnlich wirkmachtige frei verfügbare Tools, auf die einfach zugegriffen werden kann, existieren unseres Wissens derzeit nicht. Der Nachteil ist, dass diesen Tools selten eine (sozial-)wissenschaftliche Methodologie zugrunde liegt. Will heißen: Oft sind die Daten nur mit Vorsicht zu genieen, wenn eine fundierte Grundausbildung im quantitativ empirischen Arbeiten fehlt (die nicht alle kommerziellen Tools automatisch mitliefern) oder das Wissen um Kontexte und Funktionslogik digitaler offentlichkeit.

diese sehr personlichen und privaten Daten, die auch eine Rolle beim Cambridge-Analytica-Skandal spielten, sind ausdrucklich *nicht* gemeint, wenn es um – fur die offentlichkeit relevante – offentliche Daten zu politischen Debatten innerhalb der sozialen Netzwerke und den damit verbundenen Fragen zu Desinformation, Hate Speech oder alternativen Medienechokammern geht.

Welche Daten relevant waren, soll an einem einfachen Beispiel aus Facebook verdeutlicht werden:



Abbildung 1: Ein offentlicher Post der Seite „RT Deutsch“ vom 21.01.2019.

Abb. 1 zeigt einen Beitrag der Seite „RT Deutsch“ auf Facebook. In dem Beitrag ist ein Video von Donald Trump angehangt, welches auch uber den Beitrag verlinkt wird. Der Beitrag selbst ist keine Desinformation, zeigt aber ein Framing, das auch von Donald Trump gern bemuhrt wird: „Mainstream-Medien glaubt keiner mehr“. Wurde man – egal mit welchem **Social Media Intelligence Tool** – nach „Trump“ fur einen gewissen Zeitraum suchen, um beispielsweise herauszufinden, wie die Debatte in den sozialen Netzwerken uber den US-Prasidenten gefuhrt wird, wurde dieser Beitrag nicht gefunden werden, weil derzeit die dafur notige Datenschnittstelle fehlt (bzw. von Facebook nach Cambridge Analytica geschlossen wurde⁸).

Der Beitrag der Seite erschien am Montag, dem 21.01.2019, auf der Facebook-Seite der alternativen Nachrichtenplattform *RT Deutsch*, die selbst immer wieder Desinformation teilt und vom russischen Staat mitfinanziert wird.⁹ Diese Seite ist *offentlich*, das heit, dass ihre Inhalte beispielsweise uber Suchmaschinen auerhalb von Facebook oder via Suchfunktion innerhalb der Plattform zuganglich sind und jede:r Nutzer:in die Inhalte in der Plattform sehen kann. Damit sind die Daten dieser Seite aber noch lange nicht systematisch analysierbar: Dafur braucht es Datenschnittstellen, welche die Daten in sogenannte Rohdaten fur andere Softwareanwendungen uberfuhren, mit deren Hilfe zum Beispiel statistische Analysen, grafische Aufbereitungen oder thematische Suchen durchgefuhrt werden konnen. Welche Daten stecken alle in diesem Beitrag?

8 Der einzige Ausweg ware derzeit RT Deutsch als Seite „zu beobachten“. D.h. das die Seiten, die fur die Analyse interessant waren, vorher definiert werden mussen, anstatt das Facebook einfach nach Keywords uber die Datenschnittstelle durchsucht werden kann. Gerade aber bei der Logik von sozialen Netzwerken und in Bezug auf Desinformation ist a) vorneherein nicht klar, welche Seiten Desinformation teilen werden, b) ob dieser Content innerhalb der Plattform erstellt/hochgeladen wird (wie hier das hochgeladene Video) oder auerhalb der Plattform erstellt und auf den Plattformen nur geteilt wird und c) es fur jede offentliche Seite potentiell moglich ist, einen „viralen Hit“ zu landen, der Aufmerksamkeit generiert. Die Beispiele in Kapitel 3 vertiefen diese Problematik.

9 Bundeszentrale fur politische Bildung (28.06.2016): Propaganda und Desinformation. Ein Element "hybrider" Kriegfuhrung am Beispiel Russland, <http://www.bpb.de/apuz/232964/propaganda-und-desinformation?p=all>



Technische Daten:	Absender: RT Deutsch, Uhrzeit/Datum: Montag, 21.01.2019, 15:40
Bilddaten:	im Beispiel keine ¹⁰
Videodaten:	Das Video uber Donald Trump, welches unternitelt ist. Dieser Text konnte wiederum durchsuchbar gemacht werden, um Schlagworte aus dem Video ebenfalls auffindbar zu machen.
Suchergebnisdaten:	Bei welchen „Schlagworten“ taucht dieser Beitrag innerhalb der Facebook-Suchfunktion an welcher Position auf? Mit anderen Worten: Wenn sich Nutzer:innen zu Trump uber Facebook informieren, erhalten sie zuerst Vorschlage von Medien wie RT Deutsch oder von bspw. Qualitatsmedien wie Tageszeitungen oder offentlich-rechtlichen Angeboten?
Performance/ Reichweite:	Shares, Likes & Comments = „Engagement“ als Social-Media-Wahrung fur „aktive Reichweite“ sowie die Aufrufzahlen (bisher nur fur Videos verfugbar). Facebook wei auch, bei welchen Zielgruppen dieses Video erfolgreich war. Diese Daten konnten aggregiert auch fur die offentlichkeit verfugbar gemacht werden.
Metadaten:	Nicht im Beitrag sichtbar, aber theoretisch konnte dieser Beitrag von einer Fact-Checking-Organisation (fur Deutschland: Correctiv) gepruft worden sein, ob die Inhalte im Video faktisch richtig sind. Facebook hat diese Informationen fur jeden Post, sie sind jedoch bisher fur niemanden systematisch erfassbar.

¹⁰ Siehe fur den Zugang zu Bilddaten, wenn es sich mit Bilder inklusive Text handelt, Kapitel 3.

¹¹ Dieses Sichtbarmachen von anderungen – hier ist Facebook vorbildlich – sollte ein genereller Standard in der digitalen offentlichkeit werden, um Leser:innen uber Veranderungen an Texten zu informieren. Oft werden im Nachhinein auf „Nachrichten“-Seiten wie BILD oder Epoch Times Textelemente geandert und Falschinformationen im Nachhinein ausgebessert, ohne das dies fur die Nutzer:innen der Seiten sichtbar gemacht wird. Zahlreiche Beispiele hierfur finden sich auch in unserer Bundestagswahlstudie.



- Editierte Inhalte: Facebook bietet die Option an, den Bearbeitungsverlauf eines Beitrages fur jede:n Nutzer:in anzeigen zu lassen (Abb. 2). Hier lasst sich nachverfolgen, ob und wie Beitrage im Nachhinein verandert wurden. Twitter „lost“ dieses Problem, indem Tweets nach der Veroffentlichung nicht mehr bearbeitet werden konnen.¹¹ Instagram oder YouTube bieten keine solche Funktion an.
- Geloschte Inhalte: Tools wie *Talkwalker* konnen durch die Speicherung von Daten durch regelmaige Schnittstellenabfragen auch Beitrage sehen, die spater geloscht wurden. Gerade beim Thema Desinformation, gibt es immer wieder kritische Beitrage, die nachtraglich von ihren Verbreiter:innen geloscht werden – ohne, dass es fur die Nutzer:innen kenntlich ware. Uber archivierte Datenbanken sind diese Beitrage manchmal weiter auffindbar.
- Werbeanzeigen: Dieser Beitrag konnte auch von RT Deutsch als Werbeanzeige geschaltet worden sein. Die Werbebibliothek von Facebook¹² musste diese Werbung dann anzeigen und wurde dadurch transparent machen, *wer, wie viel Geld* ausgibt, um *wen* damit auf der Plattform zu erreichen.



Abbildung 2: Bearbeitungs­historie eines Facebook-Posts der BILD-Zeitung (der Case stammt aus unserer Studie "Fakten statt Fakes", in der ersten Version (08.07.) werden Falschinformationen geteilt [auf dem Bild ist weder der Tater zu sehen, noch stand zur Debatte, ob ein Beamter sein Augenlicht verliert]) – deutlich wird hier, wie die Bildzeitung falsche Informationen editiert und entfernt, die nderungen aber selbst im Post nicht kenntlich macht. Problematisch, wenn ein Groteil der Reichweite auf die Falschinformation (08.07.) entfallt – die spatere(n) Bearbeitung(en) (10.07., 12.07.) werden dabei kaum registriert. Facebooks Editi­onshistorie ist hier sehr hilfreich, die Chronologie von Desinformation herzustellen, ist aber so oder so auch kein Teil der fruher verfugbaren Schnittstellen-Daten (es handelt sich um einen Zufallsfund).

Aus der Summe solcher Daten lassen sich am Ende konkrete Fragen beantworten, die beispielsweise in Bezug auf Desinformationskampagnen von groer Bedeutung sind:

Wer teilt Desinformation? Wie viele Menschen erreichen Desinformation? Wurden diese durch Fact-Checking-Organisationen gepruft? Wie ist das Verhaltnis zwischen Desinformation und korrekten Nachrichten zum Thema XY? Werden Desinformation auch uber Werbeanzeigen geteilt und wenn ja, wie viel Geld wird darin von wem investiert, um wen damit zusatzlich zu erreichen, der u.U. diesen Seiten auf den Plattformen gar nicht folgt? Wurden falsche Inhalte nachtraglich bearbeitet? Wie werden Desinformation in sozialen Netzwerken kommentiert und vielleicht sogar debunked? Etc.

Einige dieser Fragen – aber auch nicht alle – konnten wir bspw. in unserer Studie zur Bundestagswahl 2017 zumindest fur die dort aufgefuhrten

Fallbeispiele beantworten.¹² Konkrete Informationen zur methodischen Erhebung sind zudem in einem separaten Methodenpapier zusatzlich veroffentlicht.¹³ Allerdings waren die dort beschriebenen Erhebungen derzeit nicht moglich, da, gerade bei Facebook, wichtige Datenschnittstellen (u.a. im August 2018) geschlossen wurden.¹⁴ Andere Teile dieser Daten (wie z.B. die Metadaten zum Fact-Checking oder die Untertitel innerhalb des Videos) sind bisher noch gar nicht verfugbar gewesen. Auch das systematische Erforschen von Memes und deren Verbreitung ist bisher kaum moglich.

Inwieweit die Enthullungen zu Cambridge Analytica durch die britische Zeitung The Guardian im Sommer 2018 bei der Schlieung wichtiger Datenschnittstellen durch Facebook eine Rolle gespielt haben mogen, kann hier nur gemutmat werden. Die Zeitschrift T3N dokumentiert: „Die **Media-Solutions-API** umfasst mehrere API, mit denen Tools fur Medienpartner entwickelt werden konnen. Kunftig werden API zur offentlichen Inhaltssuche auf Seiteninhalte und offentliche Posts auf bestimmten verifizierten Profilen beschrankt. Nachdem bereits verschiedene Tools dieser Familie deaktiviert wurden, folgen wegen geringer Nutzung am 1. August auch die API fur Topic Search, Topic Insights, Topic Feed und Public Figure.“¹⁵

Als „Ersatz“ wurde das reduzierte „Einhangen von Kanalen“ weiterhin ermoglicht. Das heit, dass sich thematische Suchen uber die API mittels Tools insofern durchfuhren lassen, wenn man vorher die zu durchsuchenden Kanale benennt. Im Falle der Messung von Desinformation ist es jedoch utopisch, bereits im Vorhinein abzusehen, welche Kanale wann und wie welche Desinformation teilen werden. Diese Definition im Vorhinein einer Messung festzulegen widerspricht der Natur der Sache, wie wir im Folgekapitel zu Chemnitz auch noch einmal veranschaulichen werden. Die Anzahl der beobachtbaren Kanale wird zudem auch noch durch einige Anbieter der Social Media Intelligence-Tools begrenzt.

In der Summe der Manahmen lasst sich dadurch etwa ein Viertel der Daten aus der von uns untersuchten Desinformation in der gesamten digitalen offentlichkeit nicht mehr systematisch beobachten, verglichen mit den Daten, die wir bei der Bundestagswahl erheben konnten – allein durch das Schlie-

¹² siehe Funote 4.

¹³ Wolf-Dieter Ruhl (12/2017): Measuring Fake News – Die Methode. https://www.stiftung-nv.de/sites/default/files/fake_news_methodenpapier_deutsch.pdf

¹⁴ Offizielle Ankundigung von Facebook vom 02. Juli 2018 zur Schlieung der Schnittstellen: <https://newsroom.fb.com/news/2018/07/a-platform-update/>

¹⁵ T3N (03.07.2018): „Facebook kundigt neue API-Einschrankungen fur Apps an“, URL: <https://t3n.de/news/facebook-kuendigt-neue-1092496/>



Ben der Facebook-Schnittstellen. Heit: 27 % der von uns erhobenen Daten zu Desinformation zur Bundestagswahl stammen originar aus Facebook¹⁶ und lassen sich derzeit nicht beobachten. Durch diese Verzerrung und den Wegbruch der Datenlage war es insofern auch methodisch unverantwortlich, beispielsweise eine systematische Analyse zu Desinformation wahrend der bayerischen Landtagswahl durchzufuhren – wie es unser Projektteam eigentlich vorhatte. Methodische Alternativen zu diesem Verfahren, die auch rechtlichen Rahmenbedingungen standhalten (also: kein Scrapen), gibt es derzeit unseres Wissens nach nicht.

Unabhangig davon, ist die Analyse von Social-Media-Daten ohnehin mit hohen organisatorischen und finanziellen Aufwendungen verbunden¹⁷, da offentlich zugangliche Daten, inklusive Daten aus Schnittstellen nicht existieren. Oder die Wissenschaft auf extrem teure Social Media Intelligence-Tools angewiesen ist, deren Datenbasis oft schwer nachvollziehbar ist. Das liegt auch daran, dass diese Tools vor allem zu kommerziellen Zwecken eingesetzt werden (Marketing, Marktbeobachtung, Krisenkommunikation).

Abbildung 3 fasst nun noch einmal zusammen, welche Daten, die fur Journalismus, Wissenschaft, NGOs oder andere Forschungsorganisationen einsehbar und systematisch analysier- und durchsuchbar sein mussten.

¹⁶ Berechnungen unseres Research-Partners Unicepta zur Folge.

¹⁷ Die Folge davon ist, dass es in der Wissenschaft einen gigantischen uberfluss an Twitter-Studien gibt, weil die Datenpolitik des Konzerns wesentlich offener und transparenter ist. Twitter hat allerdings in kaum einem Land die gleiche Bedeutung fur digitale offentlichkeiten, wie Facebook. Die ubertragung von wissenschaftlichen Erkenntnissen von einer Plattform zur anderen ist jedoch aus mehreren Grunden problematisch: unterschiedliches Design sowie die Funktionslogik der Plattformen spielen genauso eine Rolle wie verschiedene Zielgruppen, welche die jeweiligen Plattformen nutzen.

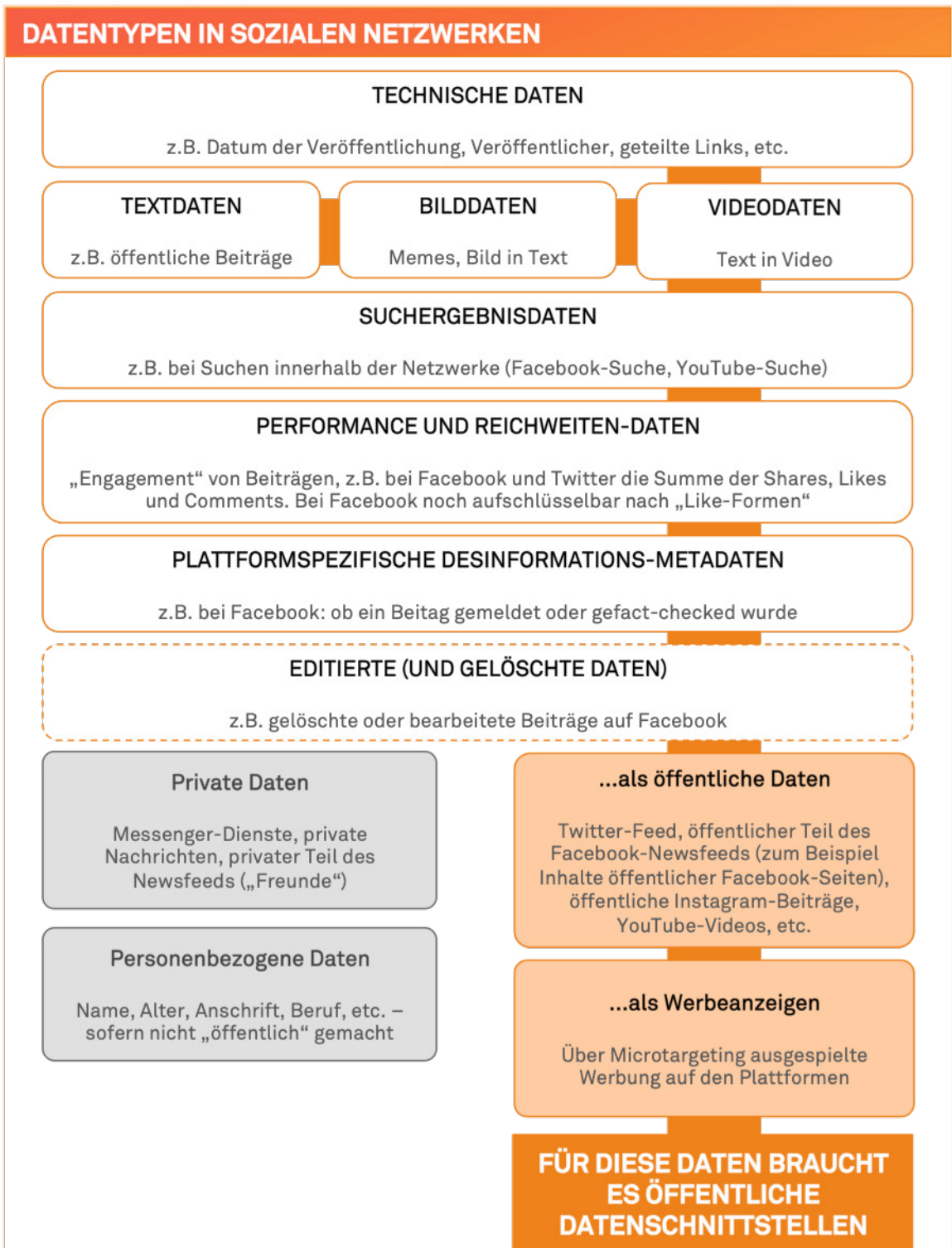


Abbildung 3: Datentypen innerhalb sozialer Netzwerke, die bspw. fur das Nachvollziehen von Desinformationskampagnen fur die offentlichkeit von Bedeutung waren.



3. Exkurs: Klaviatur der Desinformationsdaten – das Beispiel Chemnitz

In diesem Kapitel soll noch einmal die Bedeutung der Zuganglichkeit dieser Daten und Datenschnittstellen fur die offentlichkeit verdeutlicht werden.¹⁸ Dafur ziehen wir die Vorfalle in Chemnitz im August 2018 heran, da hier Desinformation in den sozialen Netzwerken einen groen Anteil an dem Ausma der Proteste und deren Organisation hatten. Viele Einzelheiten der Vorgange in den sozialen Netzwerken sind nicht etwa der Transparenz von Facebook und Co. zu verdanken, sondern der investigativen Arbeit von Journalist:innen und Fact-Checking-Organisationen. Dabei musste es nicht nur Aufgabe, sondern auch im eigenen Interesse der sozialen Netzwerke sein, solche Desinformationskampagnen zu unterbinden, damit Verschworungstheorien, Lugen und Propaganda nicht auf einen fruchtbaren Nahrboden fallen und massiv verbreitet werden. Letztlich sind soziale Netzwerke nicht immer alleiniger Auslosungsort, auch unseriose Medienanbieter und schlecht gemachter Journalismus spielen zuweilen eine Rolle¹⁹, allerdings haben die Plattformen eine Verantwortung als Transmitter und Katalysator von Desinformation.

Ausschreitungen in Chemnitz

Nach dem gewaltsamen Tod Daniel H.s in Chemnitz, in der Nacht vom 25. zum 26. August 2018, kam es in den Folgetagen dort zu Ausschreitungen durch Rechtsextreme und Neonazis, die im Anschluss in einer medialen Debatte bis hin zu Einlassungen des damaligen Leiters des Bundesamts fur Verfassungsschutz Hans-Georg Maaen endeten, ob es sich dabei um „Hetzjagden“ handle. Dabei sind viele Desinformation uber soziale Netzwerke geteilt worden, unter anderem um Menschen zu mobilisieren, an Protestzugen teilzunehmen. Unter die Demonstrant:innen mischten sich auch Rechtsextreme und Neonazis, die sich uber soziale Netzwerke verabredet hatten. Die vielen geteilten Desinformation haben wahrscheinlich zur Mobilisierung beigetra-

¹⁸ Wer bereits uberzeugt ist, kann mit Kapitel 4 fortfahren.

¹⁹ Alexander Sangerlaub/Miriam Meier/Wolf Dieter-Ruhl (2018): Fakten statt Fakes. Verursacher, Verbreitungswege und Wirkungen von Fake News im Bundestagswahlkampf 2017, <https://www.stiftung-nv.de/de/publikation/fakten-statt-fakes-verursacher-verbreitungswege-und-wirkungen-von-fake-news-im>



gen und dafur gesorgt, dass die Polizei mit der Masse der Demonstrierenden und Randalierenden uberfordert war, wie der Spiegel aufgearbeitet hat.²⁰

Die grote Reichweite erlangten dabei, sofern ohne Datenschnittstellen uberhaupt rekonstruierbar, drei konkrete Falschaussagen: 1. der Getotete wollte angeblich deutsche Frauen beschutzen, 2. es hatte noch ein zweites Mordopfer gegeben, 3. der Tater hatte den Mord vorher uber soziale Netzwerke angekundigt. Daruber hinaus gab es noch eine Vielzahl weiterer nicht korrekter Aussagen, wie eine angebliche Reisewarnung zu Sachsen aus Kanada. Alle Vorfalle und Desinformation sind sehr sorgfaltig und umfangreich von journalistischen Medien aufbereitet worden.²¹ Der Sinn der gezielt verbreiteten Falschinformation: „...um Fakten kummern sich die Urheber der zahlreichen Falschmeldungen nicht. Ihre Fake News sind Mittel zum Zweck: ‚Die Wut soll gezielt geschurt werden – und bei den geplanten Demonstrationen vom Netz auf die Strae getragen werden.‘“, schreiben Patrick Gensing und Karolin Schwarz im *Faktenfinder*.²²

Im nun Folgenden geht es weniger um eine Rekonstruktion der Ereignisse, sondern viel mehr um die unterschiedlichen Formen der Desinformation sowie der Datenlogik dahinter. Diese orientieren sich nach wie vor an der Logik von Abb. 3.

Textdaten (offentliche Beitrage)

Offentliche Beitrage sind Beitrage von Seiten, denen jede:r Nutzer:in folgen kann – unabhangig ob nun bei Facebook, Twitter oder Instagram. Deren Beitrage erscheinen dann beispielsweise im News Feed der Nutzer:innen. Die plattformubergreifende Suche nach konkreten Beitragen mittels Suchbegriffe via Tools wie Talkwalker – und sofern es sich nur um Text handelt – ist derzeit nur bei Twitter und YouTube moglich. Bei Instagram sind die Suchmoglichkeiten eingeschrankt (derzeit ist nur die Suche nach „Hashtags“ moglich). Ebenso bei Facebook funktioniert die Suche uber die Datenschnittstelle nur noch dann, wenn der Kanal vorher zur Analyse ausgewahlt wurde (womit kanalunabhangige Themenanalysen nicht moglich sind). Ganz

²⁰ SPIEGEL/SPIEGEL ONLINE (22.12.2018): Ausschreitungen in Chemnitz. Wie Politik und Polizei versagten, URL: <http://www.spiegel.de/plus/ausschreitungen-in-chemnitz-wie-politik-und-polizei-versagten-a-00000000-0002-0001-0000-000161498502> (Paywall)

²¹ Ausfuhrliche Hintergrunde finden sich dazu beispielsweise bei Patrick Gensing und Karolin Schwarz, die fur den Faktenfinder von Tagesschau.de berichteten: „Das Trauerspiel von Chemnitz“ (30.08.2018), URL: <https://faktenfinder.tagesschau.de/inland/chemnitz-fakes-trauerspiel-101.html>

²² ebd.

konkret am Beispiel: Der Beitrag der *AfD Erzgebirge* (Abb. 4) wurde nur bei Facebook mittels Tools uber die API gefunden werden konnen, wenn der Kanal „AfD Erzgebirge“ vorher als zu beobachtend ausgewahlt werden wurde. Bei der Verbreitung von Desinformation ist es aber nahezu unmoglich, vorher auszuwahlen, welche Kanale diese verbreiten oder teilen werden.



Abbildung 4: offentlicher Beitrag der AfD Erzgebirge vom 26. August 2018. Der Hinweis, dass die Opfer „Frauen helfen wollten“ ist eine Falschinformation. Bisherigen Erkenntnissen nach handelte es sich um einen Raububerfall. Auf vielen rechtsextremen Seiten wurde auch unter schlagen, dass das Opfer Deutsch-Kubaner ist.

Sonderfall: Textdaten als offentliche Beitrage privater Personen

Auch Privatpersonen konnen ihre Beitrage auf offentlich stellen, sodass sie von Nutzer:innen geteilt werden konnen. Dieses Konzept des „offentlich privaten Beitrags“ gibt es so nur bei Facebook. Auch mithilfe der nun geschlossenen Schnittstelle war es nicht moglich, diese Posts systematisch zu analysieren. Rechte Influencer:innen, aber auch Privatleute, nutzen ihre privaten Facebook-Accounts zur Verbreitung von Falschinformationen, indem sie ihre Beitrage offentlich stellen.

Hierfur zwei Beispiele (Abb. 5 & 6). Abb. 6 zeigt den privaten Account von Franz P., der ein hochgeladenes Video des rechtsnationalen Rappers Chris Ares, „mit kurzem Draht zur Identitaren Bewegung“²³, teilt.

²³ Stuttgarter Nachrichten (29.08.2018): Wie YouTube mit rechter Hetze umgeht, URL: <https://www.stuttgarter-nachrichten.de/inhalt.ausschreitungen-in-chemnitz-wie-youtube-mit-rechter-hetze-umgeht.50e2546c-505b-45b6-95be-b80d2b5b3d9d.html>



Abbildung 5: So ziemlich alles ist an diesem offentlich geteilten Post dieses privaten Nutzers falsch, auer der Nachricht, dass Daniel H. erstochen wurde. Problematisch auch, dass hier ein Bild des Opfers, wie auch einer weiteren Frau, geteilt wird – ohne auf die Privatsphere des Opfers Rucksicht zu nehmen. Der Post wurde allein knapp 20.000 mal geteilt. EDIT: Der Name des Nutzers und die Gesichter der Personen auf dem Foto wurden nachtraglich von uns verpixelt.

Ein weiterer Sonderfall ist das Kommentieren von Privatnutzer:innen von offentlichen Beitragen – diese Kommentare werden innerhalb der Plattform offentlich. Hier konnte fur den Zugriff der Wissenschaft die Namen der Kommentierenden einfach geloscht werden – wichtiger waren ohnehin nur die Inhalte der Kommentare zu offentlichen Beitragen, um zum Beispiel zu sehen, ob in den Kommentarspalten Hate Speech verbreitet wird, oder Desinformation – auch das kommt vor – durch Nutzer:innen debunked werden.



Abbildung 6: Dieses durch eine Privatperson offentlich geteilte Video, in dem der rechte Rapper Chris Ares zu den Vorfallen in Chemnitz Desinformation verbreitet, hat extrem hohe Reichweiten. Es wird alleine 111.000 geteilt, dazu kommen 20.000 Likes und 4.000 Kommentare. Facebook gibt eine Reichweite 2,6 Mio. Views an. Zum Vergleich: die erfolgreichste „Fake News“, die wir zur Bundestagswahl messen konnten, kommt – mit einer Vielzahl von Akteuren, die sie zusammen geteilt haben – auf ein Engagement von 250.000. EDIT: Name von uns verpixelt.

Videodaten

Daran anschließend kommen wir gleich zu einem der Hauptprobleme: Falschinformationen in Videos, wie dem des rechten Rappers Chris Ares, lassen sich uberhaupt nicht auffinden, wenn die Videobeschreibung den Inhalt nicht hergibt. Heißt: Der Inhalt des Videos lasst sich nicht durchsuchen, obwohl es technisch moglich ware. Wer als Fact-Checker beispielsweise herausfinden will, ob in einem Videobeitrag massiv Desinformation geteilt werden, muss ihn ganz klassisch manuell sichten. In diesem Fall konnte nur dadurch, dass das Wort „Chemnitz“ im Beitrag von Franz P. (Abb. 6) fallt, das Video uberhaupt aufgefunden werden. Der Inhalt des Videos ist nicht durchsuchbar, dennoch verbreiten sich die vielen darin getroffenen Falschaussagen in hohen Zahlen (das Video hat allein bei Facebook 2,6 Millionen Abrufe):

„In dem Clip ruft Chris Ares, der wahrend der Aufnahme in einem Auto sitzt, offen zu den rechten Protesten in Chemnitz auf und verbreitet Unwahrheiten. So sei der Anlass fur die Messerattacke, die von Rechten fur ihren Aufmarsch instrumentalisiert wurde, angeblich sexuelle Belastigung einer Frau gewesen. Außerdem spricht Ares von zwei Toten. Beides ist laut Polizei und sachsischem Innenministerium falsch.“²⁴

Das Video haben allein in den ersten Tagen bei YouTube etwa 435.000 Menschen gesehen. Sowohl Facebook als auch YouTube haben den Account von Chris Ares gesperrt. Das Video wird aber weiterhin von anderen Accounts hochgeladen (Stand: 22.12.2018 existiert noch immer eine Version auf YouTube²⁵, hochgeladen von einem Dritt-Account, ohne Hinweis, dass die Aussagen in dem Video falsch sind).


Was aber die Durchsuchbarkeit von Aussagen in Videos betrifft, sind die technischen Voraussetzungen dafur eigentlich langst gegeben, wie Abb. 2 beim RT-Beispiel und der Untertitelung Trumps zeigen: So existiert Software, die Audiospuren in Videos zu Text umwandeln kann. Diese wird sogar von YouTube bereits genutzt, wenn man Videos hochladt und diese automatisch untertiteln mochte. Damit bestehen bereits die technischen Voraussetzungen fur die Durchsuchbarkeit der Sprachinhalte der Videos und ihr mogliches Auffindbarmachen uber textbasierte Suchen.

24 ebd.

25 Video von Chris Ares auf YouTube – hochgeladen von einem Drittaccount. <https://www.youtube.com/watch?v=jxNAipkgSAI&t=21s>



Bilddaten, Gelochte Daten



Messer-Opfer
21 hrs · 🌐

Schon wieder wurde ein Mitburger erstochen und mehrere weitere schwer verletzt.
Über die Anzahl der weiteren verletzten Manner machen verschiedene Medien bisher unterschiedliche Angaben. Das Chemnitzer Stadtfest wurde nach diesem schlimmen Verbrechen inzwischen abgebrochen.

Quellen: u.a.:
https://twitter.com/BILD_Chemnitz/status/1033626398080942081 (update 27.08.: Die Bild Chemnitz hat ihren gestrigen tweet inzwischen offenbar gelocht - wir haben aber einen screenshot davon gesichert)
<https://www.wochenendspiegel.de/messerstecherei-beim-stadt.../>
<https://www.focus.de/.../toter-und-verletzte-nach-toedlichen-...>
<https://fredalanmedforth.blogspot.com/.../chemnitz-mann-beim-...>

35-jahriger Deutscher auf Stadtfest erstochen, als er einer Frau helfen wollte, die Berichten zufolge von mehreren Mannern "anderer Nationalitat" belastigt wurde.

Zwei bis drei weitere Manner, die offenbar ebenfalls zu Hilfe eilten, wurden auch niedergestochen und z.T. schwer verletzt.

Die Polizei nahm zwei Tatverdachtige fest, mochte aber deren Nationalitaten bisher noch nicht mitteilen.

Quelle u.a.: <https://www.hna.de/welt/streit-nach-stadtfest-in-chemnitz-ein-toter-mehrere-verletzte-bei-messerattacke-zr-10155494.html>

👍👎🗨️ 948 412 Comments 9.4K Shares

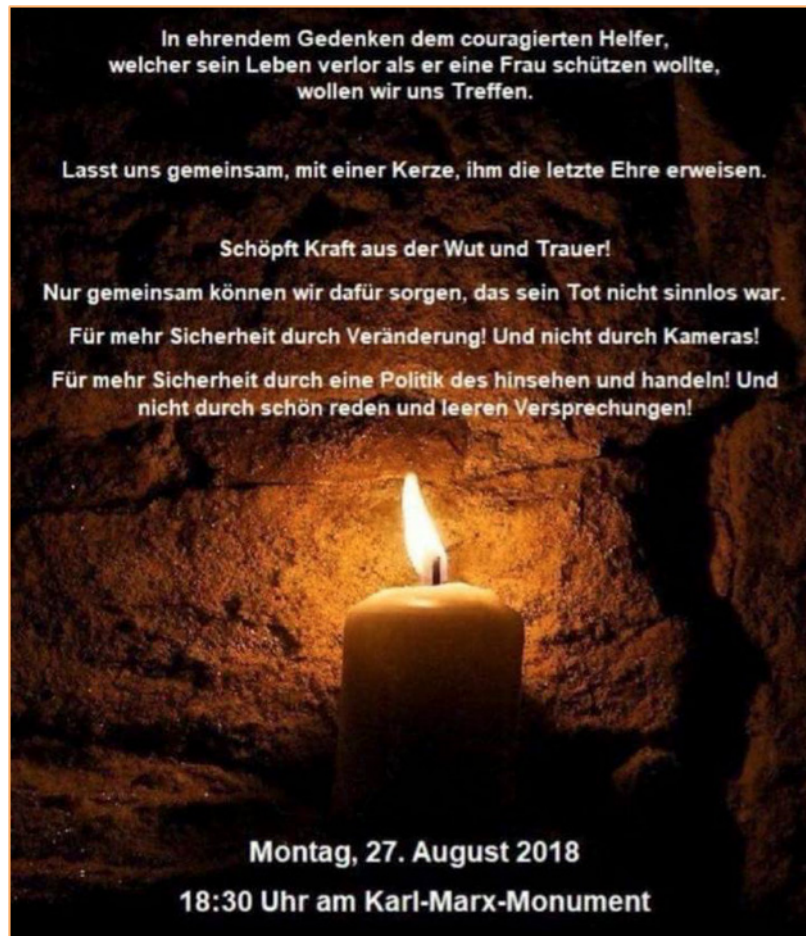


Abbildung 7 und 8: Der Text auf den beiden geteilten Bildern enthalt ebenfalls Desinformation. Der Text auf den Bildern ist allerdings nicht durchsuchbar. Auch wenn es technisch moglich ware.

Bilder sind auf den sozialen Netzwerken als Content besonders erfolgreich – das soziale Netzwerk Instagram ist sogar speziell darauf ausgerichtet, dass Bilder (und auch Videos) geteilt werden. Auch hier gibt es keine uns bekannte Moglichkeit Bilder mit oder ohne Text aufzufinden und zu analysieren.

Manuell bietet Google hierfur die beste Moglichkeit – allerdings muss dafur bereits bekannt sein, welches Bild genau gesucht wird. So ermoglicht es die Bildersuche bei Google, Bilder hochzuladen, zu denen dann Suchergebnisse angezeigt werden.²⁶ Auch fur das Auffinden geloschter Inhalte kann Google nutzlich sein, da die Google-Suchergebnisse nicht jeden Tag vollstandig aktualisiert werden. So lie sich zum Beispiel aufspuren, dass auch der Ac-

²⁶ Auch im Fact-Checking ist diese Funktion von Google sehr hilfreich. Mittels Bilderruckwartssuche lassen sich so zum Beispiel auch gefalschte Bilder aufspuren.

count von *LEGIDA* bei Facebook das Bild geteilt hatte (spater wurde dieser Beitrag auf der Seite von *LEGIDA* geloscht). Auch die rechtsnationale Band



Abbildung 9: Die Google-Bildersuche findet das Bild auch bei Facebook, dabei hat *LEGIDA* das Bild zu dem Zeitpunkt bereits bei Facebook geloscht. Es erreichte allein knapp 20.000 Likes.

FLAK hatte dieses Bild auf Facebook geteilt, aber spater wieder geloscht.

Suchergebnisdaten

Die nachste Datenform, deren systematische wissenschaftliche Analyse bisher nur durch hohen Aufwand moglichst ist, sind Suchergebnisse auf den Plattformen. Sowohl Facebook als auch YouTube stehen hier immer wieder in der Kritik in Bezug darauf, wie sie ihre Suchergebnisse anzeigen, wie **Abb. 10** exemplarisch zeigt. Im Zuge der Auseinandersetzung um die Einlassungen des damaligen Prasidenten des Bundesamts fur Verfassungsschutz, Hans-Georg Maaßen²⁷, haben wir nach Beitragen auf Facebook daruber gesucht. In den Suchergebnissen zu Videos finden sich gleich vier Videos der Alternative fur Deutschland, nur eines vom ZDF schafft es in die Top 5-Suchergebnisse.

27 Zeit Online (07.09.2018): Verfassungsschutzprasident Maaßen auert Zweifel an Hetzjagdvorwurfen, URL: <https://www.zeit.de/politik/deutschland/2018-09/verfassungsschutz-hans-georg-maassen-chemnitz-hetzjagd>



Abbildung 10: Problematisch sind auch die Suchergebnisse auf Facebook, wie auf YouTube. Suchte man Beispielsweise nach „Maaen“, bzw.

Auch der Videoplattform YouTube wird immer wieder vorgeworfen, als Radikalisierer zu wirken, da vor allem Empfehlungen des Algorithmus immer extremere Inhalte prasentieren.²⁸ Das liegt auch daran, dass besonders viele extreme Inhalte auf YouTube prasent sind, dagegen aber wenig klassische Qualitatsmedien. Auch in Chemnitz war das der Fall, wie die taz berichtete:

„Serratos Analysen sagen, dass die meisten YouTube-Videos zu Chemnitz, die in den Tagen nach den Ausschreitungen popular waren, stramm rechts waren. Und dass in der Empfehlungsspalte, die auf YouTube rechts neben dem Video auftaucht, auch dann schnell Verschworungstheoretisches und Rechtsextremes vorgeschlagen wurde, wenn man eigentlich nur nach Nachrichten zu Chemnitz gesucht hat.“²⁹

Inzwischen haben sich die Suchergebnisse zum Fall Chemnitz verandert und Medien wie *Welt*, *Bild*, *Tagesschau* und *MDR* werden angezeigt. Die Plattform arbeite an ihrem Empfehlungsalgorithmus, so die taz weiter: „Seit dem 11. September dieses Jahres hat YouTube auch in Deutschland zwei Funktionen eingefuhrt, die die Empfehlungen bei Nachrichtenthemen beeinflussen. „Breaking News“ soll dabei helfen, Falschmeldungen und unseriose Nach-

²⁸ taz (13.10.2018): Verschworungstheorien auf YouTube. Mit jedem Klick immer weiter nach rechts. URL: <http://www.taz.de/!5540029/>

²⁹ ebd.



richtenquellen bei aktuellen Groereignissen weniger prominent anzuzeigen, „Top News“ sortieren nach der gleichen Logik Nachrichten auch dann noch, wenn die Aktualitat etwas abgeebbt ist.“³⁰

Werbeanzeigen

Ob zusatzlich zur Mobilisierung von einigen Facebook-Seiten auch noch Werbeanzeigen geschaltet wurden, ist derzeit leider uberhaupt nicht nachvollziehbar, denn Facebooks Werbibliothek enthalt derzeit keine Daten fur Deutschland. Doch auch wenn diese freigeschaltet wurde, ware es derzeit unklar, ob Posts, die zu einer Mobilisierung aufrufen wurden, unter die von Facebook definierte Kategorie von *Politischer Werbung* fielen. Dann mussten sich die Werbetreibende vorher freischalten lassen, um entsprechende Werben zu veroffentlichen.

4. Wie diese Daten zur Verfugung gestellt werden konnten

4.1 Datenschnittstellen

Wir fassen zusammen: Um Desinformationskampagnen systematisch zu untersuchen, braucht es eine Vielzahl von Daten. Nur die wenigstens davon stellen die Plattformen bisher uber Datenschnittstellen oder Transparenztools fur Wissenschaft, Journalismus, NGOs oder die offentlichkeit vollumfanglich zur Verfugung. *Abb. 11* gibt einen abschlieenden uberblick, wie es um die Datenschnittstellen derzeit bestellt ist. Was unter den jeweiligen Datentypen zu verstehen ist, wurde in *Kap. 2 & Abb. 3* erlautert. Deutlich wird: Zu vielen Daten existieren nur eingeschrankt funktionierende Datenschnittstellen oder gar keine. Den besten Zugang zu Daten bietet im Vergleich noch Twitter, wodurch es allerdings auch in der Wissenschaft einen massiven uberschuss von Studien zu Twitterdaten gibt.

³⁰ ebd.















































FUR WELCHE DATEN GIBT ES BRAUCHBARE DATENSCHNITTSTELLEN?				
				
TECHNISCHE DATEN				
TEXTDATEN				
BILDDATEN				
VIDEODATEN				
SUCHERGEBNIS-DATEN				
PERFORMANCE- & REICHWEITEN				
DESINFO-METADATEN				
EDITIERTE BEITRAGE				
GELO SCHTE BEITRAGE				
WERBEANZEIGEN				

Abbildung 11: Fur welche Datentypen gibt es brauchbare Datenschnittstellen? Rot = keine Schnittstelle vorhanden, gelb = Schnittstelle nur eingeschrankt oder nicht vollstandig (Beispiel: Werbeanzeigenregister – bisher nur fur die USA bei Google bzw. fur USA/GB/BRA/IND bei Facebook). Grun = Schnittstelle vorhanden. Grau = trifft nicht zu (bei YouTube gibt es keine Bilder) oder: nicht einschatzbar. Die Beurteilung beruht auf der Einschatzung von Anbietern von Social Media Intelligence, Datenjournalisten und dem SNV-Team. Alle abgetragenen Daten beziehen sich nur auf offentliche Daten. Inwiefern es sinnvolle Schnittstellen fur *geloschte* oder *editierte* Beitrage geben kann, muss im Einzelfall fur die jeweiligen Netzwerke diskutiert werden.

Werden Daten von den Plattformen doch bereitgestellt, sollten vergangene Daten nicht erst durch langwierige und komplizierte Antragsverfahren an nur eine Handvoll Wissenschaftler:innen ubergeben werden, wie es Facebook derzeit mit *Social Science One*³¹ betreibt. Auch, weil die sich bewerbenden Institutionen sehr dezidiert Auskunft geben mussen, welche Daten sie genau

31 Webseite von <https://socialscience.one/>

zu welchen Forschungsfragen auswerten wollen. Ein so umstandliches Verfahren widerspricht der Dringlichkeit des Erkenntnisgewinns und der Logik induktiver Verfahren und ist ebenso hinderlich fur alle Institutionen, die ein sinnvolles Echtzeit-Monitoring durchfuhren mussen, wie z.B. Fact-Checking-Organisationen oder zivilgesellschaftliche Organisationen, die Desinformation oder Hate Speech beobachten.³²

Im Idealfall funktionieren demnach beides ein Echtzeit-Monitoring von sozialen Netzwerken – wie es Fact-Checking-Organisationen oder NGOs benotigen, aber auch der Zugriff auf vergangene Daten durch die Wissenschaft, die im Nachhinein dann versucht, zu rekonstruieren, wie beispielsweise die Debatte zum UN-Migrationspakt in den sozialen Netzwerken entstanden ist. Dabei konnen zuweilen auch geloschte Daten wichtig sein, wie es im konkreten Fall von Chemnitz ebenfalls deutlich wurde.

4.2 Transparenztools

Im Idealfall geht die Transparenz weit uber die Datenschnittstellen hinaus, sodass es auch fur die offentlichkeit moglich ist ohne Social-Media-Intelligence-Anbieter oder ausgewiesene Programmierkenntnisse, die offentlichen Debatten in sozialen Netzwerken systematisch nachzuverfolgen. Dafur brauchte es ein Transparenztool, das beispielsweise (politische) Themen durchsuchbar macht und aufbereitet – und diese Daten aber auch im Hintergrund als Schnittstelle fur eigene Auswertungen bereit halt.

Was utopisch klingt, ist mit den **Wahlwerberegistern**³³ von Facebook und Google bereits einigermaen funktionierende Realitat und kann als Blaupause fur andere Transparenztool herangezogen werden, auch gibt es eine Datenschnittstelle.³⁴ Allerdings gibt es auch hier Einschrankungen in der

32 Facebook stellt journalistischen Institutionen und Fact-Checking-Organisationen auf Antrag das Tool Crowdtangle zur Verfugung. Laut Aussagen uns bekannten Organisationen, die mit dem Tool arbeiten, bestehen hier aber die gleichen Probleme durch die Einschrankung der Datenschnittstellen.

33 Wahlwerberegister. Facebook nennt dieses Tool „Werbebibliothek“, diese ist (Stand: 22.01.2019) bisher fur die USA, Grobritannien und Brasilien verfugbar: https://www.facebook.com/ads/archive/?active_status=all&ad_type=political_and_issue_ads&country=ALL, Google nennt seine ubersicht „Politische Werbung bei Google“, diese enthalt bisher (Stand 22.01.2019) nur die USA: <https://transparencyreport.google.com/political-ads/overview>

34 Fur das Wahlwerberegister bei Facebook („Werbebibliothek“) existiert eine solche Schnittstelle: <https://www.facebook.com/ads/archive/access>



Funktion und einen langen ‘Leidensweg’ bis zur Verwirklichung, der sich so nicht wiederholen sollte:

Die Wahlwerberegister sind die Transparenzpolitische Antwort von Google und Facebook auf einen nun schon uber fast drei Jahre andauernden Prozess. Dahinter stehen zwei Fragen: 1) Welchen Einfluss hatten auf den Plattformen geschaltete Werbeanzeigen (fruher: als sogenannte *Dark Ads*) auf die US-Wahlen oder den Brexit³⁵ und 2) inwiefern haben welche (auslandische) Akteure sich in Wahlen und Referenden eingemischt, indem u.a. auch gezielte Desinformationskampagnen geschaltet wurden (z.B. durch die Alt-Right-Bewegung beim Referendum zu Schwangerschaftsabbruchen in Irland³⁶). Fragen, die sich in Bezug auf Desinformationskampagnen auf den Social-Media-Plattformen ebenfalls stellen – auch ganz ohne, dass sie als ‘Werbeanzeigen’ ausgespielt werden.



Abbildung 12: Politische Werbung bei Google – Transparenzbericht mit Benutzeroberflache. Bisher funktionstuchtig fur die USA. URL: https://transparencyreport.google.com/political-ads/overview?top_advertisers=q:obama&lu=top_advertisers

35 Correctiv (06.08.2018): ‘Dark Ads’ bei Facebook: Wie mit Falschnachrichten Stimmung fur den Brexit gemacht wurde. <https://correctiv.org/faktencheck/hintergrund/2018/08/06/dark-ads-bei-facebook-wie-mit-falschnachrichten-stimmung-fuer-den-brexite-gemacht-wurde/>

36 Netzpolitik (25.05.2018): Irland: Mit Dark Ads gegen Abtreibung. <https://netzpolitik.org/2018/irland-mit-dark-ads-gegen-abtreibung/>



Abbildung 13: Werbebibliothek fur Facebook und Instagram. Bisher funktionstuchtig fur USA, Grobritannien und Brasilien. URL: https://www.facebook.com/ads/archive/?active_status=all&ad_type=political_and_issue_ads&country=ALL

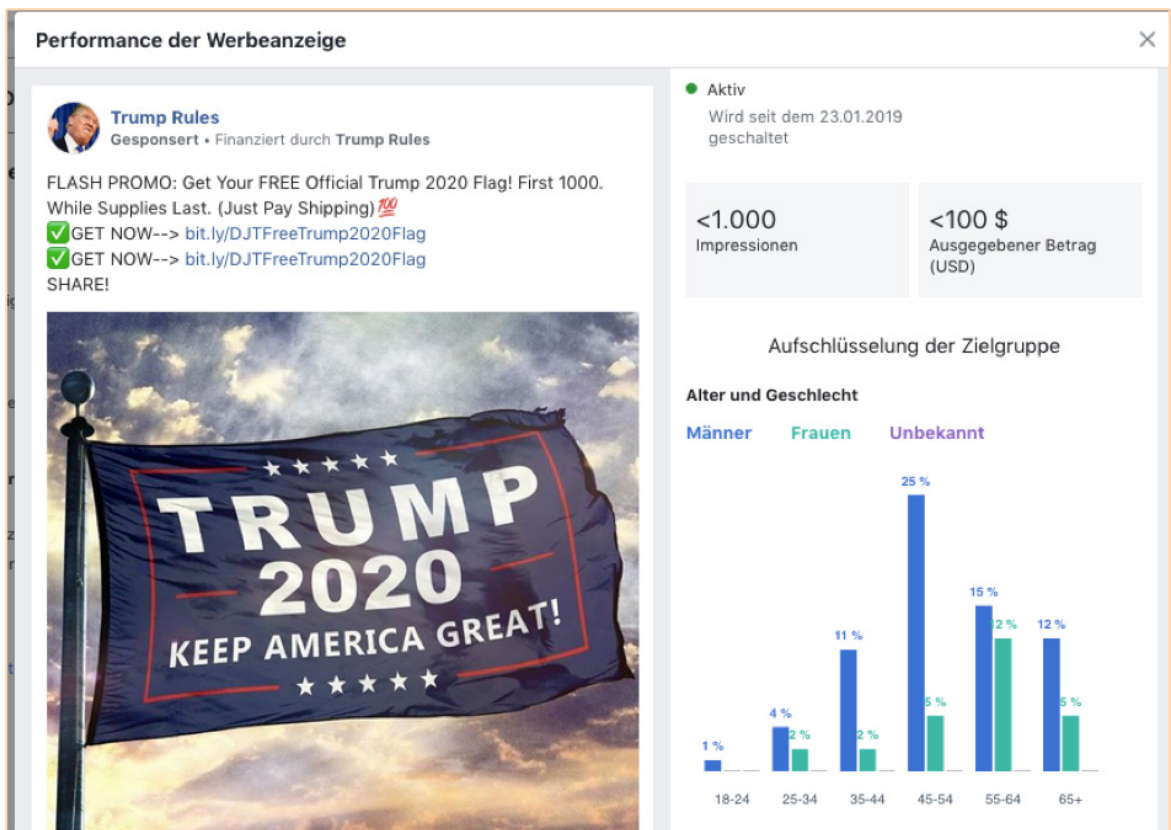


Abbildung 14: Beispiel fur Transparenz in der Werbebibliothek bei Facebook. Angezeigt werden auch Informationen uber den Financier des Posts, wie viel Geld investiert wurde, in welchem Zeitraum der Post online ist/war und die Zielgruppen.

Die Wahlwerberegister ermoglichen nun – unabhangig von der Datenschnittstelle – auch der interessierten offentlichkeit die Moglichkeit der „Selbstbeobachtung“. Diese Moglichkeit ist sicherlich der richtige Weg hin zu transparenten Kommunikationsprozessen in den digitalen offentlichkeiten, bergen aber dennoch einige Schwachstellen, die nicht unerwahnt bleiben sollen, weil sie auch die Komplexitat zwischen “gut gemacht” und “gut gemeint” aufzeigen. So existieren diese Transparenztools bei Google bisher nur fur die USA, beziehungsweise bei Facebook nur fur die USA, Brasilien, Indien und Grobritannien. Allerdings steht die Europawahl vor der Tur: Fur die 27-EU-Staaten warten alle Beteiligten noch immer auf die Freischaltung der Wahlwerberegister, die von beiden Konzernen angekundigt wurde.

Eine weitere Schwachstelle ist die derzeitige Regelung dazu, welche Anzeigen in die Datenbanken aufgenommen werden. So hat beispielsweise *ProPublica* mit einem eigenen Tool Werbeanzeigen der *National Rifle Association (NRA)* finden konnen, die nicht in Facebooks Werbebibliothek fur Amerika erscheinen³⁷ – obwohl sie es als “politische Werbung” oder “Themen nationalen Interesses” tun mussten. Problem dahinter: Damit Werbeanzeigen in Facebooks Werbebibliothek angezeigt werden, mussen sich Werbetreibende selbst kategorisieren, ob sie “politische Werbung” oder “Themen von nationalem Interesse” bewerben. Tun sie dies nicht, tauchen ihre Anzeigen auch nicht auf. Anstatt das Facebook mit ProPublica zusammenzuarbeiten, um ein effizienteres Schwachstellenmanagement zu betreiben, wurde das genutzte Tool durch eine anderung im Code von Facebook unbrauchbar gemacht – auch das zeigt Facebooks Umgang mit Akteur:innen die versuchen, an Daten zu kommen und diese auszuwerten. **Andere werden wiederum vor Gericht gezogen, weil sie gegen Facebooks eigene Datenrichtlinien verstoen.**

4.3 Politik oder Plattformen: Einer muss sich bewegen

Ob der Zugang zu offentlichkeitsrelevanten und offentlichen Daten freiwillig durch die sozialen Netzwerke erfolgt oder Regulierer hier weisend eingreifen mussen, soll hier nicht Thema sein. Mit Hinblick auf die kommenden Wahlen – von der Europawahl im Mai dieses Jahres bis zu den drei Landtagswahlen in Deutschland im Herbst – besteht allerdings dringender Handlungsbedarf. Die Befurchtungen der Wahlmanipulation durch gezielte Propaganda und Falschinformationen kommen schlielich aus der Erfahrung der US-Wahlen und dem Brexit-Volksentscheid. Gerade die undurchsichtige Gemengelage von 27 EU-Staaten mit eigenen, spezifischen Mediensystemen, geopoliti-

³⁷ Foreign Policy (01.06.2018): How Ireland Beat Dark Ads

<https://foreignpolicy.com/2018/06/01/abortion-referendum-how-ireland-resisted-bad-behaviour-online/>



schen Einflussen in- und auerhalb der EU, verschiedener Mediennutzung und Freiheitsgrade innerhalb der Mediensysteme machen es dringend notwendig, die Vorgange in den Plattformen transparent und offentlich zu machen.

Naturlich tragen die sozialen Netzwerke nicht „die Schuld“ an der Wahl Trumps oder am Brexit – diese Gleichung ist unzulassig, weil sie unterkomplex und verkurzt ist, aber doch immer wieder Teil der offentlichen Debatte. Die Disruptionen und Transformationen des Mediensystems, werden aber ihren Anteil zu einer komplexen Gleichung von politischen, gesellschaftlichen und okonomischen Faktoren tragen, die wir nach wie vor noch zu wenig verstehen.

Es scheint unabdingbar, dass wir als Gesellschaft ein tiefes und dezidiertes Verstandnis von der Wirkungsweise sozialer Netzwerke erlangen. Dafur brauchen aber Wissenschaft, Journalismus, NGOs und Zivilgesellschaft, als Beobachter dieser neu entstehenden digitalen Teiloffentlichkeiten, Zugang zu Daten. Und diese systematische Beobachtung ist nur moglich, wenn funktionierende Datenschnittstellen bereitgestellt und Transparenztools fur die offentlichkeit geschaffen werden.

Das Anliegen des Autors dahinter ist es, mehr Forschung, mehr kritische Beobachtung und mehr Verstandnis fur die digitalen offentlichkeiten der Netzwerke zu ermoglichen, die weder vom Wohlwollen der sozialen Netzwerke abhangig sind, noch hohe technische oder kommerzielle Hurden setzen und die sensible und private Daten schutzen. Auch gute Medienpolitik ist auf diese Daten dringend angewiesen. Im Datenzeitalter leben die Digitalkonzerne davon, unsere Daten massenweise zu sammeln und fur eigene Geschaftszwecke zu verwenden. Es wird Zeit, diese Daten mit der Gesellschaft zu teilen.



Alexander Sangerlaub

Marz 2019

Der blinde Fleck digitaler offentlichkeiten

Uber die Stiftung Neue Verantwortung

Think Tank fur die Gesellschaft im technologischen Wandel

Neue Technologien verandern Gesellschaft. Dafur brauchen wir rechtzeitig politische Antworten. Die Stiftung Neue Verantwortung ist eine unabhangige Denkfabrik, in der konkrete Ideen fur die aktuellen Herausforderungen des technologischen Wandels entstehen. Um Politik mit Vorschlagen zu unterstutzen, fuhren unsere Expertinnen und Experten Wissen aus Wirtschaft, Wissenschaft, Verwaltung und Zivilgesellschaft zusammen und prufen Ideen radikal.

Uber den Autor



So erreichen Sie den Autor

Vorname Name

Projektleiter Projektname

mail@stiftung-nv.de

+49 (0)30 81 45 03 78 80



Impressum

Stiftung Neue Verantwortung e. V.

Beisheim Center
Berliner Freiheit 2
10785 Berlin

T: +49 (0) 30 81 45 03 78 80

F: +49 (0) 30 81 45 03 78 97

www.stiftung-nv.de

info@stiftung-nv.de



Design:

Make Studio

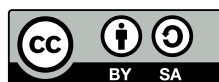
www.make-studio.net

Layout:

Johanna Famulok

Free Download:

www.stiftung-nv.de



Dieser Beitrag unterliegt einer CreativeCommons-Lizenz (CC BY-SA). Die Vervielfaltigung, Verbreitung und Veroffentlichung, Veranderung oder ubersetzung von Inhalten der Stiftung Neue Verantwortung, die mit der Lizenz „CC BY-SA“ gekennzeichnet sind, sowie die Erstellung daraus abgeleiteter Produkte sind unter den Bedingungen „Namensnennung“ und „Weiterverwendung unter gleicher Lizenz“ gestattet. Ausfuhrliche Informationen zu den Lizenzbedingungen finden Sie hier:

<http://creativecommons.org/licenses/by-sa/4.0/>