ISD | Institute for Strategic Dialogue

gefördert durch:
Auswärtiges Amt

Datenzugang zu Social-Media-Plattformen für die Forschung:

Lehren aus bisherigen Maßnahmen und Empfehlungen zur Stärkung von Initiativen inner- und außerhalb der EU

Sara Bundtzen & Christian Schwieter

Über das Digital Policy Lab

Als zwischenstaatliche Arbeitsgruppe engagiert sich das Digital Policy Lab (DPL) dafür, politische Lösungen zur Verhinderung und Bekämpfung der Verbreitung von Desinformation, Hassrede sowie extremistischen und terroristischen Inhalten im Internet aufzuzeigen. Die Arbeitsgruppe besteht aus Vertreter:innen der zuständigen Ministerien und Aufsichtsbehörden ausgewählter liberal-demokratischer Länder. Die Arbeit des DPL zielt darauf ab, den regierungsübergreifenden Dialog zu fördern, politischen Entscheidungsträger:innen und Aufsichtsbehörden Zugang zu einschlägigem Fachwissen und Forschungsergebnissen zu verschaffen sowie eine internationale Arbeitsgemeinschaft zur Bewältigung der wichtigsten digitalpolitischen Herausforderungen aufzubauen. Wir danken dem Auswärtigen Amt für die Unterstützung des Projekts.

Über diesen Bericht

Im Rahmen des DPL organisierte das Institute for Strategic Dialogue (ISD) zwischen Oktober und November 2022 mehrere Arbeitsgruppentreffen zum Thema Datenzugang. Die Arbeitsgruppe bestand aus Vertreter:innen nationaler Ministerien und Aufsichtsbehörden aus Frankreich, Großbritannien, Irland, Kanada, der Schweiz, der Slowakei und den USA. Zu den Teilnehmer:innen gehörten zudem Vertreter:innen der Zivilgesellschaft, der Wissenschaft und der Industrie. Dieser Bericht baut auf den Diskussionen auf und vertieft sie. Auch wenn die Teilnehmer:innen an diesem Bericht mitgewirkt haben, spiegeln die darin geäußerten Ansichten nicht unbedingt die Ansichten aller Teilnehmer:innen oder der an diesem Projekt beteiligten Regierungen wider.

Autor:innen

Sara Bundtzen ist Analystin bei ISD Germany. Sie erforscht die Verbreitung von Desinformation und Informationsmanipulation durch staatliche und nichtstaatliche Akteur:innen im deutschen und englischen Sprachraum. Im Rahmen des Digital Policy Lab (DPL) unterstützt sie die digitalpolitische Arbeit des ISD und untersucht Vorschläge zur Bekämpfung von Desinformation, Einflusskampagnen, Hassrede und extremistischen Inhalten.

Christian Schwieter ist Fellow beim ISD und promoviert im Fachbereich Medienwissenschaften an der Universität Stockholm, wo er die Auswirkungen der europäischen Plattform-Governance-Bemühungen auf rechtsextreme Aktivitäten in sozialen Medien untersucht. Bis 2023 war er Project Manager bei ISD Germany und leitete das vom deutschen Justizministerium geförderte mehrjährige Forschungsprojekt »Radikalisierung in rechtsextremen Online-Subkulturen entgegentreten«. Zuvor war er Co-Leiter der Pilotphase des Digital Policy Lab (DPL) am ISD.

Herausgeberische Verantwortung
Huberta von Voss, Executive Director ISD Germany

Danksagungen

Unser ausdrücklicher Dank gilt den Teilnehmer:innen aus der Zivilgesellschaft, der Wissenschaft und der Industrie sowie allen Mitwirkenden an diesem Bericht für ihre wertvollen Einblicke, ihre Kritik und ihr Feedback: Ľuboš Kukliš (ehemals Council for Media Services), Oliver Marsh (The Data Skills Consultancy), Chris Meserole (The Brookings Institution), Nina Morschhäuser (ehemals Twitter Deutschland), Susan Ness (Annenberg Public Policy Center), Chris Riley (Annenberg Public Policy Center), Jack Pay (CASM Technology), Mathias Vermeulen (AWO Agency), und Dr. Katrin Weller (GESIS). Darüber hinaus nahmen auch Mitarbeiter:innen von Meta an der Arbeitsgruppe teil und trugen durch ihr Feedback zu dieser Veröffentlichung bei.

ISD | Institute for Strategic Dialogue

www.isdgermany.org

Inhaltsverzeichnis

Executive Summary

Dieser Bericht gibt einen Überblick über die Erkenntnisse, die aus der bisherigen Zusammenarbeit zwischen Industrie und Forschung sowie anderen bereits bestehenden Initiativen zum Thema Datengang hervorgegangen sind. Die vorliegende Untersuchung befasst sich darüber hinaus mit potenziellen zukünftigen Möglichkeiten der internationalen Zusammenarbeit zwischen liberal-demokratischen Staaten, wobei der Schwerpunkt auf den Rahmenwerken für Regulierung und Ko-Regulierung auf EU-Ebene liegt. Der vorliegende Bericht enthält spezifische Empfehlungen für Plattformen, Forscher:innen, Aufsichtsbehörden sowie Regierungsinitiativen in Bezug auf eine Harmonisierung der theoretischen Ansätze und praktischen Handlungsoptionen.

Empfehlungen zur Gewährleistung der öffentlichen Aufsicht von Social-Media-Plattformen und des Zugriffs auf Plattformdaten für die im öffentlichen Interesse liegende Forschung.

Erarbeitung gemeinsamer Methoden zur Datenerfassung und Datendokumentation:

- Forscher:innen, die im öffentlichen Interesse liegende Forschung betreiben, und Aufsichtsbehörden sollten Grundsätze und Praktiken für das Datenmanagement festlegen, um die Reproduzierbarkeit, Überprüfbarkeit und Peer Reviews von Forschungsergebnissen zu ermöglichen.
- Forscher:innen und Aufsichtsbehörden sollten anwendbare Vergleichswerte entwickeln, die eine plattformübergreifende und komparative Betrachtung des Nutzungsverhaltens und von Inhalten ermöglichen.
- Um ein besseres Verständnis der breiteren gesellschaftlichen Auswirkungen der sozialen Medien zu erreichen, sollten die Aufsichtsbehörden den Wert von Forschungsansätzen mit kombinierten Methoden berücksichtigen, einschließlich verschiedener Methoden zur Datenerhebung, die bei der im öffentlichen Interesse liegenden Forschung angewendet werden.

Verbesserung der Transparenzberichterstattung:

- Unternehmen, Aufsichtsbehörden und Forscher:innen, die im öffentlichen Interesse tätig sind, sollten für mehr Konsistenz und Standardisierung der Transparenzberichterstattung sorgen, indem sie eine Reihe gemeinsamer Metriken und Kategorien entwickeln, wo immer dies sinnvoll ist. Wenn es aufgrund unterschiedlicher geografischer, sprachlicher und rechtlicher Kontexte keine eindeutigen Kategorien für Inhalte gibt, sollten die Plattformen die Methodik zur Kategorisierung der Inhalte transparent machen.

Gewährleistung des sicheren Zugriffs auf maschinenlesbare Daten durch Forscher:innen mit Zustimmung der Unternehmen:

- Unternehmen und politische Entscheidungsträger:innen sollten sicherstellen, dass bei der Regelung des Datenzugangs ein differenzierter und nuancierter Ansatz angewandt wird, der die unterschiedlichen Erwartungen der Nutzer:innen an den Datenschutz berücksichtigt. Öffentliche Daten, bei deren Verarbeitung keine »vernünftigen Erwartungen« betroffener Personen an den Datenschutz zu berücksichtigen sind – beispielsweise Inhalte, die auf öffentlichen Seiten oder in öffentlichen Gruppen gepostet werden oder Inhalte von Persönlichkeiten des öffentlichen Lebens –, sollten über einen zulassungsbeschränkten Zugang zu Programmierschnittstellen (*Application Programming Interface, APIs*) verfügbar gemacht werden und Metriken für Reichweite (*reach*), Impressionen (*impressions*) und Interaktion (*engagement*) beinhalten.
- Unternehmen sollten eine umfassende öffentliche Dokumentation über berechtigte Anwendungsfälle und Forschungsanforderungen für den Zugriff auf *API*-Endpunkte bereitstellen. Dabei sollte eindeutig angegeben werden, welchen Zugriff Forscher:innen über die *API* erhalten können und welche Arten von Anwendungsfällen zulässig sind.
- Aufsichtsbehörden und Forscher:innen sollten kritisch hinterfragen, warum Unternehmen die Abfrage historischer Daten oder das Datenvolumen einschränken. Die Aufsichtsbehörden sollten die Unternehmen um Klarstellung dieser einschränkenden Maßnahmen bitten und sie gegebenenfalls beanstanden können, wenn diese die im öffentlichen Interesse liegende Forschung beeinträchtigen.

Gewährleistung einer sicheren Nutzung von Crowdsourcing-Daten und Datenspenden durch Forscher:innen:

- Politische Entscheidungsträger:innen sollten die Forscher:innen rechtlich schützen, damit diese Plattformen unter Einhaltung angemessener Datenschutzvorkehrungen untersuchen können.
- Unternehmen sollten in den Nutzungsbedingungen ihrer Plattformen freiwillige Ausnahmeregelungen

vorsehen, um Crowdsourcing und Datenspenden über Browsererweiterungen zu Forschungszwecken zu ermöglichen. Eine Voraussetzung hierfür ist, dass die Forscher:innen sich an die Datenschutz-Grundverordnung (DSGVO) der EU halten, einschließlich der Einholung einer aufgeklärten Zustimmung der Teilnehmer:innen. Dies könnte den Plattformen gegenüber beispielsweise durch eine Genehmigung einer zuständigen Forschungsethikkommissionen nachgewiesen werden.

Harmonisierung der Datenschutzanforderungen in den verschiedenen Rechtssystemen:

- Politische Entscheidungsträger:innen in EU- und Nicht-EU-Ländern sollten die bestehenden Datenschutzregelungen der europäischen DSGVO anwenden, insbesondere die spezifischen Ausnahmen in Bezug auf die Verarbeitung zu im öffentlichen Interesse liegenden Archivzwecken und zu wissenschaftlichen Forschungszwecken.
- In diesem Zusammenhang sollten grenzübergreifende Kooperationen auf dem Entwurf eines Verhaltenskodex für die gemeinsame Nutzung von Plattformdaten für die im öffentlichen Interesse liegende Forschung aufbauen, der von der Arbeitsgruppe der Europäischen Beobachtungsstelle für digitale Medien (*European Digital Media Observatory, EDMO*) entwickelt wurde.

Ermöglichung von Zulassungsverfahren für Forscher:innen außerhalb des regulatorischen Rahmens:

- Politische Entscheidungsträger:innen und Aufsichtsbehörden sollten Gesetzeslücken für den unbefugten Zugriff auf Daten durch Privatunternehmen, Regierungs- oder Strafverfolgungsbehörden schließen. Zugelassenen Forscher:innen wäre es somit verboten, Daten für kommerzielle Zwecke zu nutzen oder diese Daten an unbefugte Dritte weiterzugeben.
- Auch wenn die Zugehörigkeit zu einer akademischen Einrichtung als Gatekeeper-Funktion dienen kann, sollten auch nicht-akademische Forscher:innen, die im öffentlichen Interesse tätig sind, zugelassen werden.
- Politische Entscheidungsträger:innen und Aufsichtsbehörden sollten die grenzübergreifende Anwendung von Zulassungsmechanismen zur Vorabüberprüfung von Forscher:innen eindeutig regeln. Neben den im Entwurf des Verhaltenskodex der *EDMO* enthaltenen Vorschlägen sollte die Vereinheitlichung und Integration der Verfahren einen Schwerpunkt der internationalen Zusammenarbeit bilden.
- Politische Entscheidungsträger:innen, Aufsichtsbehörden und Unternehmen sollten anerkennen, dass Zeit ein wichtiger Faktor bei Forschungsprojekten sein kann und diese auf den rechtzeitigen Zugriff auf Daten angewiesen sind. Die Bearbeitung von Anträgen auf Datenzugang könnte an den Krisenreaktionsmechanismus des Gesetzes über digitale Dienste (*Digital Services Act, DSA*) der EU angeglichen werden.
- Politische Entscheidungsträger:innen und Aufsichtsbehörden sollten Zulassungsmechanismen nicht nur der Einhaltung von Vorschriften wegen in Erwägung ziehen, sondern auch aus Gründen einer im öffentlichen Interesse liegenden Forschung. Neben der Untersuchung von Desinformation und »systemischen Risiken« sollten Zulassungen für Datenzugänge auch für im öffentlichen Interesse liegende Forschungsprojekte offenstehen, die darauf abzielen, die Auswirkungen sozialer Medien auf die Gesellschaft als Ganzes zu verstehen.

Schaffung einer unabhängigen Vermittlungsstelle:

- Um Interessenskonflikte zu vermeiden und eine umfassende demokratische Aufsicht zu gewährleisten, sollten die Aufsichtsbehörden sicherstellen, dass eine unabhängige vermittelnde Stelle (*independent intermediary body*) selbst bestimmte Transparenzstandards einhält.
- Eine vermittelnde Stelle sollte über ausreichendes wissenschaftliches und technisches Fachwissen verfügen, einschließlich der erforderlichen personellen Ressourcen, damit diese in der Lage ist, die Forschungsziele, die methodischen und ethischen Standards sowie die technischen und operativen Datenschutzvorkehrungen zu beurteilen.
- Politische Entscheidungsträger:innen, Aufsichtsbehörden und Forscher:innen sollten eine länderübergreifende Strategie für die Vermittlungsstelle fördern. So könnte die Stelle – unter Berücksichtigung der Datenschutzregelungen der DSGVO – Verzeichnisse von öffentlich zugänglichen Daten bereitstellen, die von Forscher:innen außerhalb der EU genutzt werden können. Sie könnte beispielsweise einen zentralen öffentlichen Speicher für Datenkataloge und Codebücher bereitstellen, in denen spezifiziert und erläutert wird, welche Arten von Social-Media-Daten für die Forschung verfügbar sind.

Einleitung

Die Gewährleistung eines sinnvollen Zugriffs auf Social-Media-Daten für im öffentlichen Interesse liegende Forschungsprojekte muss die Grundlage aller evidenzbasierten digitalpolitischen Initiativen bilden, die darauf abzielen, sicherere und offenere Online-Umgebungen zu schaffen. Die Beziehungen zwischen Technologieunternehmen, staatlichen Instanzen, Forscher:innen und der Öffentlichkeit sind jedoch nach wie vor durch ein hohes Maß an Informationsasymmetrie gekennzeichnet, wobei sowohl die Regelungen für den Datenzugang als auch die entsprechende Infrastruktur unzureichend sind.

Neue Vorschriften für den Datenzugang in und außerhalb der EU sollten dazu beitragen, diese Asymmetrie zu überwinden, indem sie Forscher:innen, die im öffentlichen Interesse liegende Forschungsziele verfolgen, ein besseres Verständnis über die Inhalte und das Nutzungsverhalten auf Social-Media-Plattformen ermöglichen. Um eine faktenbasierte politische Debatte sowie die Implementierung und Durchsetzung von rechtlichen Rahmenbedingungen zu ermöglichen, ist ein umfassenderes Verständnis der Art und Weise, wie Social-Media-Plattformen die öffentlichen Diskurse prägen können, von entscheidender Bedeutung.

Dabei muss die Erforschung der Rolle und des Einflusses von Plattformen auf gesamtgesellschaftliche Entwicklungen, die durch die Verbreitung von Fehl- und Desinformation, Hassrede sowie verschwörungsideologischen und extremistischen Inhalten gefährdet sind, vertieft werden. Wissenschaftler:innen wie Nate Persily weisen darauf hin, dass der Zugriff auf Social-Media-Daten zur Voraussetzung für die Untersuchung und das Verständnis der meisten zeitgenössischen Probleme »in der realen Welt« geworden ist[1] – sei es im Kontext von Wahlen, der Einflussnahme ausländischer Akteur:innen, gesundheitspolitischer Fragen, sowie gesellschaftlichen Stimmungsbildern beispielsweise in Bezug auf Klimawandel, Migration oder der Rechte von LGBT+ Personen.

Die Aussagen von Whistleblowern unter Berufung auf entsprechende offengelegte Unterlagen legen die Vermutung nahe, dass Unternehmen wie Meta in der Vergangenheit nicht immer wirksame Maßnahmen gegen individuelle oder gesellschaftliche Risiken von Online-Gefahren ergriffen haben, auch wenn sie durch ihre eigenen Mitarbeiter:innen auf diese aufmerksam gemacht worden sind.[2] Zwar veröffentlichen die meisten Social-Media-Plattformen in irgendeiner Form Transparenzberichte. Dabei zielen diese zum Teil auf die Einhaltung gesetzlicher Vorschriften[3] ab, bieten jedoch noch kein vollständiges, ganzheitliches und vergleichbares Verständnis von Werbung, Inhaltsmoderation und algorithmischen Empfehlungssystemen.

Die Forschungsgemeinschaft kämpft nach wie vor mit zahlreichen Hindernissen, die eine systematische Untersuchung der Plattformsysteme und -praktiken erschweren. Die dabei bestehenden Hürden können sich sowohl auf technologische Merkmale der Plattformen als auch auf ethische und rechtliche Bedenken in Bezug auf den Datenschutz oder die Fragmentierung von Inhalten und Nutzer:innen-Aktivitäten (und damit von Daten) auf verschiedenen Teilen der Plattformen beziehen, die deren systematische und Längsschnitts-Untersuchung einschränken. In diesem Zusammenhang merkte Philipp Lorenz-Spreen vom Max-Planck-Institut für Bildungsforschung an: »Wir sind nicht auf die Ölindustrie angewiesen, um CO_2 messen zu können, aber wir sind auf Facebook angewiesen, um die Polarisierung auf Facebook zu messen.«[4] Spätestens nach dem Skandal um *Cambridge Analytica* haben besonders die Bedenken über die Verletzung der Privatsphäre der Nutzer:innen den Aufbau der notwendigen Infrastruktur für den Zugriff auf und die gemeinsame Nutzung von Social-Media-Daten ausgebremst.

Ein umfassender Datenzugriff auf Plattformen im gesamten Online-Ökosystem würde unabhängige Aufsichtsmöglichkeiten ermöglichen, wobei die Rahmenbedingungen für den Datenzugang die Einhaltung der Datenschutzrechte der Nutzer:innen unbedingt gewährleisten müssen. Wenn diese Bedingungen erfüllt sind, kann ein reglementierter Datenzugang für Forscher:innen die demokratische Entscheidungsfindung verbessern und gleichzeitig sicherstellen, dass regulatorische Eingriffe sowohl zweckmäßig als auch verhältnismäßig sind und keine grundrechtsgefährdenden Präzedenzfälle geschaffen werden.

Der vorliegende Bericht verfolgt drei Zielstellungen:

1. Auswertung der wichtigsten Erkenntnisse, die aus der bisherigen Zusammenarbeit zwischen Industrie und Forschung sowie anderen bestehenden freiwilligen Initiativen hervorgegangen sind.
2. Auslotung potenzieller künftiger Optionen für die internationale Zusammenarbeit zwischen liberal-demokratischen Staaten, insbesondere im Rahmen der transatlantischen Partnerschaft, mit schwerpunktmäßiger Betrachtung der Rahmenwerke für die Regulierung und Ko-Regulierung auf EU-Ebene.
3. Ausarbeitung gezielter Empfehlungen für Regierungsinitiativen in Bezug auf eine Harmonisierung ihrer Ansätze in Theorie und Praxis.

Erkenntnisse aus der bisherigen Zusammenarbeit zwischen Industrie und Forschung

In Forschungskreisen der verschiedener Fachdisziplinen existieren Vorschläge für unterschiedliche Fragestellungen, deren Untersuchung bisher dadurch erschwert wird, dass Social-Media-Plattformen keinen ausreichenden Zugriff auf nutzergenerierte Daten sowie auf Plattformdaten über Moderations- und Empfehlungssysteme, Prozesse und Ergebnisse ermöglichen.[5]

Hinter der Forderung nach einem Zugriff auf Plattformdaten zu Forschungszwecken steht die Auffassung, dass diese stellvertretend zur Erklärung verschiedener gesellschaftlicher Phänomene sowie menschlicher Verhaltensweisen, Einstellungen oder Meinungen herangezogen werden könnten. Während traditionelle sozialwissenschaftliche Methoden retrospektiv angelegt sind, liefern Datensätze aus sozialen Medien zunehmend in Echtzeit umfassende aktuelle Erkenntnisse, insbesondere in Krisensituationen wie Pandemien.

Dieser Abschnitt beleuchtet die methodischen und ethischen Fragen im Zusammenhang mit dem Zugriff auf und der Verarbeitung von Social-Media-Daten, die Bewertung der Relevanz von Social-Media-Daten für Forschungszwecke und das Entstehen verschiedener Datenzugriffsmethoden im Rahmen der Forschung. Dabei werden die bestehenden Transparenzstrukturen – insbesondere die Transparenzberichterstattung durch die Plattformen – sowie die Partnerschaften und die praktische Zusammenarbeit zwischen Tech-Unternehmen und Forschungseinrichtungen untersucht.

Social-Media-Daten als Gegenstand einer im öffentlichen Interesse liegenden Forschung

Zunächst soll eine umfassende Erörterung der unterschiedlichen Datenkategorien erfolgen, die für unterschiedliche wissenschaftliche Zwecke benötigt werden. Dadurch soll den politischen Entscheidungsträger:innen und Aufsichtsbehörden ausreichendes Hintergrundwissen – insbesondere in Bezug auf Fragen des Datenschutzes – vermittelt werden. Zivilgesellschaftliche Organisationen und wissenschaftliche Einrichtungen sollten dabei klar darlegen, warum die Plattformdaten benötigt werden, zu welchen Zwecken sie verwendet werden und inwieweit ihre Forschung im öffentlichen Interesse liegt. Dies könnte wiederum die Ausgestaltung, Umsetzung und Durchsetzung der Plattformregulierung beeinflussen. Um zu verdeutlichen, welcher Zusammenhang zwischen bestimmten Daten in Abhängigkeit von der Art des Datenzugangs besteht, lassen sich mit Schwerpunkt auf der im öffentlichen Interesse liegenden Forschung die folgenden Datentypen definieren und kategorisieren:

- **Nutzergenerierte Daten** (user-generated data) umfassen Informationen über die Aktivitäten der Nutzer:innen auf einer Plattform. Theoretisch zählen dazu alle von Nutzer:innen erstellten Inhalte wie Beiträge und Kommentare sowie Informationen über Nutzersignale, einschließlich Likes, Shares und andere Arten der Interaktion mit Inhalten (Engagement). Diese Daten können sowohl öffentlicher (z. B. ein öffentlich geteilter Beitrag oder ein Kommentar unter einem öffentlichen Beitrag) als auch privater (z. B. ein Beitrag, der in privaten, kleineren geschlossenen Gruppen oder Gruppenchats geteilt wird) Natur sein. Gegenwärtig ermöglichen mehrere sehr große Online-Plattformen (*Very Large Online Platforms, VLOPs*) den strukturierten Datenzugriff auf diese öffentlichen Daten über Programmierschnittstellen (*Application Programming Interfaces, APIs*). Diese Daten sind nicht ausschließlich nutzergeneriert, sondern können auch beschreibende Statistiken über die Reichweite von Beiträgen enthalten, wie beispielsweise die Anzahl der Aufrufe oder Impressionen eines Beitrags.
- **Von den Plattformen kuratierte Daten** (platform curation data) umfassen Informationen darüber, wie Plattformsysteme nutzergenerierte Inhalte auf einer Plattform unter Einbeziehung menschlicher und algorithmischer Ressourcen moderieren und mittels eines Rankings einstufen (z. B. herauf- oder herabstufen). Dazu gehören Informationen über die Community-Richtlinien der Plattform (Richtlinien zur Inhaltsmoderation) sowie die Maßnahmen zu ihrer Durchsetzung – beispielsweise durch Entfernen oder Herabstufen von Inhalten oder Sperren von Konten. Derzeit enthalten die von den Unternehmen veröffentlichten Transparenzberichte neben zusammengefassten Informationen über Entscheidungen zur Inhaltsmoderation gelegentlich auch Angaben zur Art des Inhalts, zur Erfassungsmethode, zur Art der angewendeten Einschränkungen und zur Frage, ob die Entfernung oder die Aussetzung aufgrund der Nutzungsbedingungen, rechtlicher Anforderungen oder behördlicher Aufforderungen erfolgte.[6] Diese Art von Informationen liegt normalerweise in einem nicht maschinenlesbaren Format vor. Auf granularer Ebene könnten die von Plattformen kuratierten

Daten Signale oder Tags enthalten, die mit Arten von Inhalten oder Konten verbunden sind und für interne Systeme zur Inhaltsmoderation verwendet werden.[7]

- Zu den **Entscheidungsfindungsdaten der Plattformen** (platform decision-making data) gehören Informationen über die internen Entscheidungsprozesse der Unternehmen, einschließlich der Entscheidungen über die Plattformarchitektur, die von den Ranking-Teams durchgeführten Experimente oder die zur Auswertung der Unternehmensmetriken verwendete Methodik. Diese Daten enthalten zum Beispiel Informationen über die Verwendung von algorithmischen Empfehlungssystemen – einschließlich in Bezug auf Änderungen, die darauf abzielen, bestimmte Arten von Engagement oder Inhalte zu verstärken –, sowie die Einführung von neuen Funktionen. Solche Daten können quantitativer Natur sein, zum Beispiel das Ergebnis von Experimenten mit Ranking-Systemen. Informationen über die Methodik und Entscheidungsfindung sind dagegen in qualitativer Form zugänglich. Forscher:innen wären hier auf die Zusammenarbeit mit Mitarbeiter:innen oder der Unternehmensleitung angewiesen, entweder im Rahmen von Inspektionen vor Ort und Befragungen oder durch Zugang zu internen Dokumenten, Entscheidungsprozessen und Kommunikationsdaten. Die sogenannten ›Twitter Files‹ sind ein Beispiel für die Offenlegung derartiger Informationen, wenngleich Vorbehalte hinsichtlich ihrer Selektivität und Überprüfbarkeit bestehen.[8]

Ausgehend von bereits vorliegenden Forschungsergebnissen und der oben vorgenommenen Kategorisierung für Social-Media-Daten gibt die Tabelle 1 einen beispielhaften Überblick über einige typische aktuelle Forschungsfragen von öffentlichem Interesse. Diese unterstreichen die Sichtweise, dass der Datenzugang für wissenschaftliche Zwecke sich nicht allein durch die Einhaltung rechtlicher Vorschriften rechtfertigen sollte. Die im öffentlichen Interesse liegende Forschung kann auch Fragestellungen umfassen, die nicht in den Rahmen aktueller digitalpolitscher Debatten fallen, die aber dennoch unser Wissen über menschliches Verhalten und die Gesellschaft im Allgemeinen erweitern und dazu beitragen können, politische Entscheidungen in sonstigen Bereichen außerhalb der Regulierung von Online-Diensten zu treffen. Die Regelungen für den Datenzugang sollten daher berücksichtigen, dass die wissenschaftliche Erforschung sozialer Medien nicht nur dann von öffentlichem Interesse ist, wenn sie direkt in die Digitalpolitik und die Regulierung von Social-Media-Plattformen einfließt. Die Tabelle unterscheidet dabei zwischen Fragestellungen, die unmittelbar mit der Plattformegulierung zusammenhängen, und allgemeineren Forschungsfragen.

	Direkter Zusammenhang mit der Einhaltung von gegenwärtigen Vorschriften zur Plattformregulierung	**Indirekter Zusammenhang mit der Einhaltung von gegenwärtigen Vorschriften zur Plattformregulierung**
Erfordert primär Zugriff auf nutzergenerierte Daten	Wie weit verbreitet sind Inhalte auf Facebook, die nach dem deutschen Strafgesetzbuch als »Volksverhetzung« eingestuft werden könnten? (Bezug: Netzwerkdurchsetzungsgesetz – NetzDG) Wie viele Aufrufe haben Videoclips der Sendetätigkeiten von RT und Sputnik einen Monat vor und einen Monat nach der russischen Invasion in der Ukraine auf YouTube verzeichnet? (Bezug: restriktive Maßnahmen der EU gegen die Sendetätigkeiten der staatseigenen Medien RT und Sputnik)	Wie unterscheiden sich die Debatten über die COVID-19-Pandemie auf Facebook und Twitter? Welche Online-Nachrichten werden von deutschsprachigen Influencer:innen auf Instagram am häufigsten geteilt?

Erfordert primär Zugriff auf von Plattformen kuratierte Daten	Wie wirksam sind Warnhinweise von unabhängigen Faktenprüfer:innen oder anerkannten Quellen bei der Eindämmung der Verbreitung von Fehlinformation auf Twitter? [9] (Bezug: Verpflichtung Nr. 21 des neuen gestärkten Verhaltenskodex der EU von 2022 zur Bekämpfung von Desinformation) Welche Gruppen von Nutzer:innen sind mit größerer Wahrscheinlichkeit von Hassrede betroffen? [10] (Bezug: Verhaltenskodex der EU zur Bekämpfung illegaler Hassreden im Internet) Sind bestimmte Gruppen von den Entscheidungen der Inhaltsmoderation auf Plattformen unverhältnismäßig stark betroffen? (Bezug: UK Online Safety Bill, Abschnitt 12 über Pflichten zur Stärkung der Selbstbestimmung erwachsener Nutzer:innen) Verstärken die Algorithmen hinter der Instagram Explore-Seite systematisch die Sichtbarkeit von missbräuchlichen Inhalten? (Bezug: Basic Online Safety Expectations gem. Australia's Online Safety Act 2021) Wie hoch ist der Anteil sogenannter ›Superuser‹, die sich auf Facebook hyperaktiv und missbräuchlich verhalten? Wie lässt sich der Einfluss von ›Superusern‹ auf algorithmische Empfehlungssysteme messen? (Bezug: Gesetz über digitale Dienste der EU, Artikel 34 – Risikobewertung)	Wie wirken sich die historischen Daten zum Nutzungsverhalten auf die Empfehlungsalgorithmen von YouTube Shorts aus? Welche Rolle spielt die Feedback-Schleife zwischen Nutzer:innen-Verhalten und algorithmischen Empfehlungen? Wie ändern Nutzer:innen ihr Posting-Verhalten als Reaktion auf veränderte Funktionen einer Plattform (z. B. wie hat sich das Engagement der Nutzer:innen verändert, als Facebook die sogenannte Wütend-Reaktion einführte? Inwieweit beeinflusst die Angabe der Quelle bei Faktencheck- Interventionen die Wahrscheinlichkeit der Weiterverbreitung von Fehlinformationen durch Nutzer:innen?[11] Wird die Verbreitung irreführender Informationen durch den zusätzlichen Kontext von Beiträgen wie z. B. den Community Notes von Twitter eingedämmt? Inwieweit finden Menschen mit unterschiedlichen Standpunkten diese hilfreich? Verändert die Entscheidung für einen umgekehrt chronologischen Feed gegenüber einem algorithmischen Feed die ›Stickiness‹ von Social-Media-Plattformen, d. h. verbringen Nutzer:innen dadurch also mehr oder weniger Zeit auf einer Plattform?
Erfordert primär Zugriff auf Entscheidungsfindungsdaten der Plattformen	Werden sogenannte High-Profile-Nutzer:innen bei der Inhaltsmoderation bevorzugt behandelt? (Bezug: Gesetz über digitale Dienste der EU, Artikel 15 -Transparenzberichtspflichten) Benachteiligen die Empfehlungsalgorithmen von TikTok gezielt Aktivist:innen von ›Black Lives Matter‹, indem sie die Häufigkeit reduzieren, mit der ihre Videos im ›Für Dich‹-Feed angezeigt werden? (Bezug: Gesetz über digitale Dienste der EU, Artikel 37 – Unabhängige Prüfung) Sind Nutzer:innen in der Lage, andere zum Schweigen zu bringen, sei es durch den Missbrauch von Moderationsmechanismen oder durch systematische Schikane, die darauf abzielt, bestimmte Standpunkte zu zensieren? (Bezug: UK Online Safety Bill, 95 – Investigations, 96 – Power to require interviews, 97 – Powers of entry, inspection and audit)	Ist es möglich, eine quantitative Schätzung des Anteils an der Reichweite und des Engagements zu erstellen, der auf eine ›algorithmische Verstärkung‹ zurückzuführen ist? Wie könnten Plattformen und Forscher:innen das Verhalten der Nutzer:innen in einem ›kontrafaktischen‹ Szenario bewerten, z. B. durch den Vergleich von Nutzergruppen, die mit algorithmischen bzw. mit umgekehrt-chronologischen Feeds interagieren?[12] Wie werden die Entscheidungen von Metas Oversight Board von der Unternehmensführung aufgenommen? Welche Auswirkungen haben diese Entscheidungen auf die Praxis der Inhaltsmoderation anderer Unternehmen? Wie entscheiden die Ranking- und Produktteams der Social-Media-Plattformen über Experimente, mit denen sie Änderungen an den Algorithmen testen und bewerten und wie wenden sie diese an?

Tabelle 1: Überblick von Forschungsfragen, die direkt oder indirekt mit der Einhaltung von Vorschriften zur Plattformregulierung zusammenhängen. Dabei schließen sich die Kategorien nicht gegenseitig aus.

Die Forschungsfragen sind Beispiele für Themenfelder, die den Zugriff auf Daten erfordern, um die Auswirkungen von Social-Media-Plattformen auf menschliche Interaktionen, das individuelle Verhalten und die Gesellschaft als Ganzes erfassen und verstehen zu können. Wenngleich der im öffentlichen Interesse liegenden Forschung verschiedene Methoden zur Verfügung stehen, um auf Daten der Social-Media-Plattformen zugreifen und diese untersuchen zu können, gibt es bei der Durchführung von systematischen, langfristigen und groß angelegten Studien gewisse Hindernisse (beispielsweise in Bezug auf die Nachverfolgung des Verhaltens von Nutzer:innen über lange Zeiträume).

Hindernisse beim Datenzugang

Plattformen setzen mitunter gezielt Technologien ein, um den Zugriff auf Daten einzuschränken, oder verfügen über andere technische Funktionen, die den Datenzugang unbeabsichtigt erschweren. So sind beispielsweise bestimmte Inhaltsformate, vor allem Audio- oder audiovisuelle Inhalte, (noch) nicht in dem Maß für eine systematische Suche und Speicherung geeignet wie Text. In anderen Fällen bieten Plattformen Dienste mit Ende-zu-Ende-Verschlüsselung an, bei denen eine systematische Datenerfassung nur möglich ist, wenn der Absender oder der Empfänger den Zugriff auf die Daten gewährt. Auch das Aufkommen der Blockchain-Technologie kann weitere Hürden mit sich bringen. Die systematische Erfassung von Daten aus Blockchain-basierten Plattformen wurde bisher noch kaum erforscht. Da die zum Teil auf der Blockchain-Technologie basierenden Plattformen wie Odysee nicht über *APIs für Forschungszwecke verfügen, ist noch unklar, welche Daten verfügbar sein werden und ob beim Prozess der Datenerhebung weitere Schwierigkeiten aufkommen könnten.*[13]

Zusätzliche Hürden können im Zusammenhang mit der Fragmentierung von Daten entstehen, wenn sich relevante öffentlich zugängliche Inhalte in riesigen Datenmengen verbergen, die nicht schnell und systematisch über plattformweite Suchfunktionen oder *APIs* erfasst werden können. Die öffentlichen Gruppen von Discord können beispielsweise nur Server für Server und nicht auf systematische Weise ausgewertet werden.[14] Hinzu kommt, dass die Plattformen auch verschiedene Metriken mit unterschiedlichen Definitionen verwenden können. So können die einzelnen Plattformen unterschiedlich definieren, was unter einem individuellen Aufruf (*view*) zu verstehen ist, und was mithilfe dieser Kennzahl konkret gezählt wird. Schon allein deshalb ist es schwierig, Verhaltensweisen und Inhalte plattformübergreifend zu vergleichen und die Beobachtungen zu validieren.[15]

Auch aus der Verwendung von Fremdanbieter-Technologien zur Erfassung von Nutzer:innen-Daten (z. B. *Scraper* oder Browser-Erweiterungen) können sich rechtliche Einschränkungen ergeben, wenn sie nach den Nutzungsbedingungen der Plattformen unzulässig sind. Außerdem kann es zu Problemen mit der Aufbewahrung der Daten seitens der Plattform-Unternehmen sowie bei Forschungsbedarf in Bezug auf gelöschte Daten kommen, insbesondere wenn die Daten aufgrund eines Verstoßes gegen die Nutzungsbedingungen der jeweiligen Plattform entfernt wurden. Untersuchungen gelöschter Inhalte könnten erforderlich werden, wenn diese beispielsweise Beweise für Kriegsverbrechen in Konfliktgebieten enthalten könnten. Rechtliche Hürden können beim Zugriff auf gelöschte Inhalte auch dann entstehen, wenn gesetzliche Bestimmungen die Unternehmen dazu verpflichten, gelöschte Daten von der Aufbewahrung auszuschließen oder es ihnen verbieten, rechtswidrige Inhalte herauszugeben.

Darüber hinaus können sich aus unterschiedlichen datenschutzbezogenen Erwartungen der Nutzer:innen und Unsicherheiten in Bezug auf die Unterscheidung zwischen öffentlichen und privaten Online-Räumen ethische Probleme ergeben. Wenn beispielsweise Forscher:innen einer WhatsApp-Gruppe beitreten, können sie den gesamten Chatverlauf problemlos als Textdatei exportieren. In diesem Fall werden verschiedene ethische Bedenken aufgeworfen: Wie ist der Forscher oder die Forscherin in die Gruppe gekommen? Wurde von allen Mitgliedern die ausdrückliche Erlaubnis eingeholt, die Inhalte der Gruppe für Forschungszwecke zu verwenden (was bestimmte Teilnehmer:innen zu einer Selbstzensur veranlassen könnte)? Sind sich die Gruppenmitglieder der Anwesenheit der Forscherin oder des Forschers in ihrem Chat nicht bewusst und sind daher möglicherweise keine einwilligungsfähigen Forschungsteilnehmer:innen? Hat sich die Forscherin oder der Forscher womöglich durch Täuschung Zugang zur Gruppe verschafft?

Vor dem Hintergrund dieser vielfältigen Erschwernisse haben Forscher:innen verschiedene Forschungsmethoden

und -ansätze eingesetzt, um Social-Media-Daten zu erfassen und auszuwerten. So können die Forscher:innen beispielsweise Nutzer:innen befragen oder Sockenpuppen-Accounts verwenden, um Funktionen aus deren Perspektive mit unterschiedlichen Merkmalen zu untersuchen. Auch der Einsatz bestimmter Datenspende-Tools ist möglich, sodass Nutzer:innen freiwillig Daten direkt für wissenschaftliche Zwecke zur Verfügung zu stellen. Alternativ können Forscher:innen auch versuchen, Daten von einer Plattform abzugreifen. Beispielsweise war es über Dienste wie ScrapeHero mithilfe von *Web-Scraping möglich, historische Twitter-Daten abzurufen. Dabei riskieren die* Forscher:innen allerdings, gegen Nutzungsbedingungen der Plattformen zu verstoßen.[16] Ein weiterer Ansatz zur Datenerhebung ist die digitale Ethnographie. Dahinter verbirgt sich die Anwendung bewährter soziologischer Forschungsmethoden, die eine tiefe und langfristige Auseinandersetzung mit bestimmten Bevölkerungsgruppen beinhalten. Hierbei verfolgen die Forscher:innen einen ›menschlicheren‹ Ansatz, indem sie Online-Räume weniger als virtuelle, sondern als soziale Räume betrachten und durch Teilnahme beobachten. Dieser Ansatz zielt nicht darauf ab, größere Datenmengen zu produzieren, wie sie für quantitative Methoden erforderlich sind, und eignet sich besser für die Untersuchung von Nischen-Subkulturen, die einen immersiven Ansatz erfordert.[17]

Eine weitere Folge eines eingeschränkten Datenzugangs ist, dass in der Social-Media-Forschung insbesondere im Kontext von Studien über Fehl- und Desinformation[18] oft keine gemeinsamen Qualitätsstandards für die Datenerhebung und die Dokumentation existieren. Da eine systematische Dokumentation in der Praxis nicht existiert, leiden die Ergebnisse häufig unter mangelnder Transparenz und Nachvollziehbarkeit. Dies wiederum verhindert, dass die Forschungsanstrengungen im Sinne einer kumulativen Forschung und anhand von Peer-Reviews der analytischen Ergebnisse effektiv gebündelt werden können.[19] Das *Governance Laboratory (GovLab)* stellte fest: »Eine der größten Herausforderungen des Datenzeitalters besteht darin, dass wir es noch immer versäumen, Daten verantwortungsvoll im Sinne das Gemeinwohls zu verwerten.«[20] Darüber hinaus wird die Entwicklung bewährter Verfahren weiterhin durch die dynamische Natur der Daten in den sozialen Medien beeinflusst, zum Beispiel durch das Aufkommen kleinerer Plattformen oder dezentraler Netzwerke wie dem *Fediverse,* bei denen die Server nicht von einem Unternehmen, sondern von einer Vielzahl von Einzelpersonen gehostet werden. Die Dezentralisierung kann zu einer zunehmenden Fragmentierung führen, die die Voraussetzungen für einen systematischen Datenzugang weiter erschwert.[21]

Empfehlungen:

- **Forscher:innen und Aufsichtsbehörden sollten gemeinsame Grundsätze, Praktiken und Methoden für das Datenmanagement festlegen, um die Reproduzierbarkeit, Überprüfbarkeit und Peer-Reviews zu ermöglichen.** Die Dokumentation der Daten sollte in einer Weise erfolgen, dass eine kritische Prüfung sämtlicher Aspekte der Erfassung, Aufbereitung, Verarbeitung, Speicherung und Weitergabe erfolgen kann.[22]

- **Forscher:innen und Aufsichtsbehörden sollten Vergleichswerte entwickeln, die eine komparative Betrachtung des Verhaltens und der Inhalte innerhalb und zwischen den Plattformen ermöglichen, um zu verstehen, welche Inhalte erfolgreich sind, und wie der Erfolg gemessen wird.** Damit ließe sich beispielsweise die Frage beantworten, wie die Gesamtzahl der Likes auf einer großen Plattform im Vergleich zur Gesamtzahl der Likes auf einer anderen, kleineren Plattform zu bewerten ist. Diese Untersuchungen könnten die Entwicklung öffentlicher Indikatoren für Vergleichswerte von Plattformdaten erleichtern.[23]

- **Aufsichtsbehörden sollten vor dem Hintergrund der großen Bandbreite an Plattformen die methodische Vielfalt der Datenerhebung anerkennen.** Neben einem automatischen Datenzugang stehen verschiedene ergänzende Methoden der Datenerhebung zur Verfügung, deren potenzieller Beitrag nicht vernachlässigt werden sollte. Hierunter fallen ethnografische Beobachtungen, das Crowdsourcing von Daten oder Umfragen unter den Nutzer:innen. Gemischte Datenerhebungsmethoden führen zu einem umfassenderen Bild der gesellschaftlichen Auswirkungen sozialer Medien, da Forscher:innen die weiterreichenden Auswirkungen der Erfahrungen der Nutzer:innen berücksichtigen und auch Aspekte der Informationsverarbeitung und Medienkonsumgewohnheiten einfließen lassen können.

Transparenzberichterstattung

Bei den von den Unternehmen veröffentlichten Transparenzberichten handelt es sich um öffentliche Berichte, die in der Regel nicht maschinenlesbare Informationen oder begrenzte quantitative Beschreibungen der von den Plattformen kuratierten Daten und der Verfahren der Plattformen zur Inhaltsmoderation enthalten. So veröffentlichen beispielsweise die Unterzeichner des Verhaltenskodex zur Bekämpfung von Desinformation der EU[24], zu denen Unternehmen wie Meta, Twitter und Google gehören, im Rahmen ihrer Verpflichtungen aus dem gestärkten Kodex von 2022 Berichte im PDF- sowie im CSV- und JSON-Format – wenn auch mit eingeschränkter Nutzbarkeit.[25]

Die Transparenzberichterstattung entstand Mitte der 2000er Jahre als Reaktion der Branche auf die Bedenken der Zivilgesellschaft hinsichtlich der Beziehungen zwischen Technologieunternehmen und staatlichen Instanzen. 2010 veröffentlichte Google als erstes großes Technologieunternehmen – damals noch unter der Bezeichnung ›*Government Requests Tool*‹ – einen Transparenzbericht, in dem das Unternehmen Angaben über staatliche Aufforderungen zur Löschung von Inhalten und Herausgabe von Nutzerinformationen machte.[26] 2018 legten Menschenrechtsorganisationen, Jurist:innen und Expert:innen aus der Wissenschaft eine Reihe von Grundsätzen vor, die zeigten, wie die Moderation von nutzergenerierten Inhalten durch Plattformen so transparent und nachvollziehbar wie möglich gestaltet werden kann. Die *Santa Clara Principles on Transparency and Accountability in Content Moderation* enthielten Empfehlungen für Plattformen, die sicherstellen sollen, dass »die Durchsetzung ihrer Inhaltsrichtlinien fair, unvoreingenommen, verhältnismäßig und unter Wahrung der Rechte der Nutzer:innen erfolgt«. Diese Grundsätze von Santa Clara wurden von zwölf Tech-Unternehmen unterzeichnet – darunter Apple, Meta, Google, Reddit, Twitter und Github.[27]

2020 veröffentlichte das Open Technology Institute des Think Tanks *New America* ein umfassendes Tracking-Tool, das anhand der von sechs Plattformen über Transparenzberichte veröffentlichten Daten die Praxis der Transparenzberichterstattung in Bezug auf die Inhaltsmoderation bewertet.[28] Dabei stellte das *Open Technology Institute* fest, dass Transparenzberichte zu branchenweiten Best Practices geworden sind. Unternehmen begreifen die Transparenzberichterstattung inzwischen als Mechanismus, mit dem sie auf den öffentlichen Druck reagieren und zeigen können, wie sie Fragen der Inhaltsmoderation angehen. Erkennbar sei dies beispielhaft an Themenbereichen wie COVID-19 oder wahlbezogene Fehl- und Desinformation. Die von Unternehmen wie Meta, Google, Twitter, TikTok und Reddit veröffentlichten Transparenzberichte enthalten Daten über eine Vielzahl von Metriken. Häufig veröffentlichte Metriken treffen Aussagen über die Menge der entfernten Inhalte, die Anzahl der gesperrten Konten oder der inhaltlichen Beanstandungen. Zusätzlich wenden die meisten Plattformen auch Metriken an, die spezifisch mit deren Dienstleistungsangebot zusammenhängen. Meta veröffentlicht beispielsweise unter der Metrik der ›Prävalenz‹ (*prevalence*) den prozentualen Anteil aller Inhaltsaufrufe, die regelwidrige Inhalte in einer bestimmten Inhaltskategorie betrafen. Weiterhin führt das Unternehmen unter der sogenannten ›*proactive rate*‹ den prozentualen Anteil der Inhalte auf, die von den unternehmenseigenen Tools selbst identifiziert und markiert werden konnten, bevor Nutzer:innen sie markierten. Die Berichterstattung anhand von Metriken erfolgt je nach Beanstandung des Inhalts unter Zuordnung zu bestimmten Kategorien (z. B. ›Hassrede‹ oder ›Terrorismus/Gewaltextremismus‹). Darüber hinaus veröffentlicht Meta mit den sogenannten *Adversarial Threat Reports* Bedrohungsberichte über die Bekämpfung gezielt agierender Gruppen wegen verschiedener Richtlinienverstöße im Zusammenhang mit koordinierten Kampagnen wie *Coordinated Inauthentic Behavior* (*CIB*), *Brigading* und massenhaften Nutzerkonten-Meldungen (*Mass Reporting*). Zu den zusätzlichen Transparenzbemühungen zählt in diesem Zusammenhang der *API*-Zugang *CrowdTangle*, der mit einer kleineren Gruppe von Forscher:innen geteilt wird, die im Falle von gezielten operativen Angriffen auf das Netzwerk sowohl quantitative als auch qualitative Analysen durchführen können, ohne manuell große Tabellen durchgehen oder nach archivierten Posts suchen zu müssen.[29]

Allerdings können willkürliche und unklare Kategorisierungen für Inhalte potenziell wertvolle Erkenntnisse verschleiern. So veröffentlicht YouTube seine Metriken über die Kategorie »Spam und irreführende Inhalte« und verschleiert damit die Informationen darüber, wie »irreführende Inhalte« moderiert werden und sich auf der Plattform verbreiten. Diese Praxis droht den Wert

der Transparenzberichterstattung zu mindern. Gleichzeitig ist eine Standardisierung von Inhaltskategorien nur bis zu einem gewissen Grad zu erreichen, da es für viele Kategorien von Meinungsäußerungen keine einheitlichen Definitionen gibt, die in allen landesspezifischen und gesetzlichen Kontexten gleichermaßen anwendbar wären. So gibt es zum Beispiel keine allgemeingültige Definition für »extremistische Inhalte« oder »sexuelle Bildinhalte«, die in allen Kontexten und für alle Dienstanbieter anzuwenden wäre.

Wenn es jedoch im alleinigen Ermessen der Plattformen liegt, über welche Arten von Inhalten sie berichten (und vor allem, über welche sie nicht berichten) und wie sie diese Angaben herleiten (welche Kennzahlen sie anwenden), besteht die Gefahr, dass einige Plattformen ihre Transparenzberichterstattung als Mechanismus nutzen, um gezielt nur solche Informationen weiterzugeben, die sie in einem unverhältnismäßig positiven Licht erscheinen lassen.

Europäische Union: Gesetz über digitale Dienste (DSA)

Die neuen horizontalen Vorschriften der EU, die im Rahmen der Verordnung über einen Binnenmarkt für digitale Dienste (*Digital Services Act, DSA*) eingeführt wurden, beinhalten weitreichende Transparenzberichtspflichten. In Artikel 15 werden die Anbieter von Vermittlungsdiensten konkret verpflichtet, »aussagekräftige und verständliche Informationen« zu folgenden Punkten bereitzustellen:

- die durchgeführte Moderation von Inhalten einschließlich der Nutzung automatisierter Werkzeuge;
- die Maßnahmen zur Schulung und Unterstützung der für die Moderation von Inhalten zuständigen Personen;
- die Anzahl und Art der ergriffenen Maßnahmen, die sich auf die Verfügbarkeit, Erkennbarkeit und Zugänglichkeit der von den Nutzer:innen bereitgestellten Informationen auswirken, aufgeschlüsselt nach der Art der rechtswidrigen Inhalte oder des Verstoßes gegen die allgemeinen Geschäftsbedingungen des Dienstanbieters, nach der zur Aufspürung verwendeten Methode und der Art der angewendeten Beschränkung.

Alle Online-Plattformen müssen in den Berichten darüber hinaus folgende Angaben machen:

- die Anzahl der von den Behörden erhaltenen Anordnungen, aufgeschlüsselt nach der Art des rechtswidrigen Inhalts;
- die Anzahl der Nutzerbeschwerden, die Grundlage dieser Beschwerden, die getroffenen Entscheidungen, die bis zur Entscheidung benötigte Mediandauer und die Anzahl der Fälle, in denen diese Entscheidungen rückgängig gemacht wurden;
- die Verwendung automatisierter Mittel zur Inhaltsmoderation, einschließlich einer qualitativen Beschreibung, einer Spezifizierung der genauen Zwecke, Indikatoren für die Genauigkeit und die mögliche Fehlerquote sowie etwaige Sicherheitsvorkehrungen.

Artikel 42 schreibt vor, dass sehr große Online-Plattformen (*Very Large Online Platforms, VLOPs*) bzw. sehr große Online-Suchmaschinen (*Very Large Online Search Engines, VLOSEs*), worunter Plattformen mit mehr als 45 Millionen monatlich aktiven Nutzer:innen in der EU fallen, über die Qualifikationen und die Sprachkenntnisse der Teams für die Inhaltsmoderation sowie über die verwendeten Genauigkeitsindikatoren, aufgeschlüsselt nach EU-Sprachen, berichten müssen.

Zusätzlich zu den oben genannten Transparenzberichtspflichten verpflichtet Artikel 40 die VLOPs und VLOSEs dazu, auf »begründetes Verlangen« eines Koordinators für digitale Dienste (d. h. einer nationalen Regulierungsbehörde) zugelassenen Forscher:innen (vetted researchers) Zugriff auf Daten zu gewähren. Im Rahmen der Einhaltung der in der Verordnung festgelegten Bestimmungen würden zugelassene Forscher:innen durch entsprechende Anträge bei den zuständigen Aufsichtsbehörden Zugriff auf Daten erhalten, um zur »Aufspürung, zur Ermittlung und zum Verständnis systemischer Risiken« beitragen.

Anmerkung: Am 17. Februar 2023 gaben Unternehmen wie Google, Meta, Microsoft, TikTok, Twitter und Snapchat ihre Nutzerzahlen bekannt. Während der DSA ab dem 17. Februar 2024 für alle digitalen Dienste gilt, unterliegen VLOPs und VLOSEs den Verpflichtungen vier Monate nach ihrer offiziellen Benennung als solche. Auf Grundlage der Nutzerzahlen hat die Europäische Kommission am 25. April 2023 die erste Gruppe von 17 VLOPs und VLOSEs benannt.[30]

Empfehlungen:

- **Unternehmen, Aufsichtsbehörden und Forscher:innen sollten die Zusammenarbeit fortsetzen und für mehr Konsistenz und Standardisierung der Transparenzberichterstattung sorgen, indem sie eine Reihe gemeinsamer Metriken und Kategorien entwickeln, wo immer dies sinnvoll erscheint.** Wenn es wegen unterschiedlicher geografischer, sprachlicher und rechtlicher Kontexte keine eindeutigen Kategorien für Inhalte gibt, sollten die Plattformen die Methodik zur Aufschlüsselung der Inhalte in Kategorien transparent machen. Diese Maßnahmen sollten auf bestehenden Modellen für die Transparenzberichterstattung aufbauen, die von der Wissenschaft und der Zivilgesellschaft entwickelt wurden.[31]

Zugriff auf maschinenlesbare Daten mit Zustimmung der Unternehmen über *APIs*

In diesem Abschnitt werden die Möglichkeiten des Zugriffs auf maschinenlesbare Daten für Forscher:innen über entsprechende Programmierschnittstellen (*APIs*) erläutert. Der Zugriff auf die Daten erfolgt dabei mit Erlaubnis durch die Unternehmen und ermöglicht es externen Programmier:innen und Forscher:innen, Daten von den Servern des Unternehmens abzurufen.[32] Für die Gewährung des Zugriffs über die *APIs* der Plattformen müssen Forscher:innen derzeit meist eine gesonderte Genehmigung beantragen. Die Antragsverfahren reichen von der Einreichung eines kurzen Formulars bis hin zur Ausformulierung eines konkreten Forschungsvorschlags (*research proposal*).

Vor dem Hintergrund der Tatsache, dass verschiedene Arten von Daten mehr oder weniger schwere Bedenken hinsichtlich des Datenschutzes aufwerfen, befasst sich dieser Abschnitt mit der aktuellen Debatte über öffentliche und private Online-Räume und deren Unterschiede. Zunächst wird der Fall des Projekts *Social Science One* beschrieben, um die daraus gezogenen Erkenntnisse darzulegen. Im zweiten Teil dieses Berichts erfolgt eine Betrachtung der Akkreditierungsverfahren für die Zulassung von Forscher:innen.

Fallstudie: Social Science One

Die am *Institute for Quantitative Social Science* der *Harvard University* angesiedelte akademische Organisation *Social Science One* ermöglicht wie kaum ein anderes Kooperationsprojekt die Untersuchung von Formen der Zusammenarbeit zwischen Sozialwissenschaftler:innen und der Privatwirtschaft. Das Projekt wurde 2018 ins Leben gerufen, um erstmals ein spezielles Modell für Kooperationen zwischen Tech-Unternehmen und Forschungsmeinschaft zu erproben. Dabei sollten Daten von Facebook mit Wissenschaftler:innen geteilt werden, um testweise die »Auswirkungen sozialer Medien auf die Demokratie« zu bewerten. Im Rahmen des Projekts wurde eine »Kommission renommierter Wissenschaftler:innen« eingesetzt, die als vertrauenswürdige Drittpartei fungieren sollte und dabei »vollen Zugriff auf die unternehmenseigenen Daten hat und den Bedarf der wissenschaftlichen Kreise kennt«.[33] Forschungsvorschläge mussten zunächst von einer universitären Ethikkommission (*Institutional Review Board)* oder einem internationalen Pendant geprüft werden und unterlagen einem Peer-Review unter der Leitung des *Social Science Research Council (SSRC)*. Zusätzlich wurden die Vorschläge durch unternehmenseigene Datenschutz- und Forschungsteams und von externen Datenschutz-Expert:innen geprüft, die von der Kommission bestimmt wurden. Die Kommission wählte unabhängig die Projektpartner aus, die »datenschutzrechtlich geschützte Daten« von Facebook erhielten.[34]

Ursprünglich bestand das Forschungsziel darin, »nahezu alle öffentlichen URLs, auf die Nutzer:innen von Facebook weltweit geklickt hatten«, offenzulegen und dabei auch anzugeben, »wann und von welchen Personengruppen diese angeklickt wurden«. Auch sollten Links berücksichtigt werden, »die von unabhängigen Faktenprüfer:innen als absichtliche Falschnachrichten bewertet wurden«.[35] Allerdings kam es bei *Social Science One* zu erheblichen Verzögerungen aufgrund von Bedenken hinsichtlich des Datenschutzes der Nutzer:innen. Der Skandal um *Cambridge Analytica* hatte gezeigt, wie viele Daten die Plattformen von Nutzer:innen sammeln und potenziell für Dritte zugänglich sind. Damals hatte ein Wissenschaftler eine Entwicklervereinbarung mit Facebook gebrochen, die den Verkauf der Daten an gewinnorientierte Unternehmen untersagte.[36] Nach dem Skandal war Facebook besorgt, die öffentliche Kritik an der Verletzung der Privatsphäre der Nutzer:innen seiner Plattform weiter zu befeuern, was das Unternehmen dazu veranlasste, lediglich einen stark reduzierten Datensatz freizugeben, dessen wissenschaftlicher Nutzen deswegen unter den ursprünglichen Erwartungen lag.

Letztendlich enthielt der Datensatz Informationen über 38 Millionen URLs, die zwischen Januar 2017 und Juli 2019 mehr als 100-mal öffentlich auf Facebook geteilt wurden. Um die sensiblen Daten zu schützen, wandte Facebook den Anonymisierungsmechanismus *Differential Privacy* an, obwohl der Datensatz bereits auf URL-Ebene aggregiert war, einschließlich der aggregierten Daten über die Arten von Personen, die diese Links angesehen, geteilt, geliked, darauf reagiert und anderweitig mit ihnen interagiert haben.[37] *Social Science One* erklärte in diesem Zusammenhang, dass der Datenschutz nach dem Prinzip von *Differential Privacy* »durch die Zensierung bestimmter Werte in den Daten und das Hinzufügen von speziell kalibriertem Rauschen zu statistischen Ergebnissen oder Datenzellenwerten« angelegt sei, um »die Handlungen einer Person, die in den Daten ablesbar sein könnte«, zu verschleiern.[38] Die Projektverantwortlichen versuchten zwar, die daraus resultierenden statistischen Probleme[39] zu lösen, stellten jedoch fest, dass die meisten Ergebnisse, die aus dem Datensatz abgeleitet wurden, »mit größerer Unsicherheit behaftet waren, als wenn die Forscher:innen Zugriff auf die Originaldaten gehabt hätten«.[40] Darüber hinaus gab es Bedenken hinsichtlich der Reliabilität der Daten selbst. Datenwissenschaftler:innen von Facebook stellten fest, dass der Datensatz mit den URL etwa ein Drittel der US-Bevölkerung nicht erfasst hatte. Insbesondere enthielt der Datensatz keine Nutzer:innen, für die Facebook keine politische Gesinnung identifiziert hatte, sodass wahrscheinlich viele Menschen aus der politischen Mitte und andere Menschen, deren politische Ansichten schwer einzuordnen waren, vernachlässigt wurden.[41] Nate Persily, Mitbegründer von *Social Science One*, sieht die Erfahrungen mit dem Projekt als »einen klaren Anlass zur Schaffung eines gesetzlich gesicherten und geregelten Prozesses, der Forscher:innen Zugriff gewährt und gleichzeitig die staatliche Aufsicht zum Schutz der Privatsphäre der Nutzer:innen sicherstellt«.[42]

Zugang zu öffentlichen Daten

Wie das Projekt *Social Science One* zeigte, hat die Definition für »öffentliche Daten« im Zusammenhang mit Datenzugangsregelungen Auswirkungen auf die potenziellen Datenschutzrisiken für die Nutzer:innen, wenn diese Daten für Forschungszwecke im öffentlichen Interesse einem breiteren Personenkreis zugänglich gemacht werden. Datenzugangsregelungen müssen daher die Frage berücksichtigen, an welche Inhalte hohe Erwartungen an den Schutz der Daten der Nutzer:innen gestellt werden. Plattformen können mehrere Merkmale, Funktionen und Angebote wie Livestreaming, Seiten oder öffentliche Gruppen anbieten, die jeweils ein unterschiedliches Maß an Öffentlichkeit implizieren.[43]

Nach derzeitigen Regulierungsvorhaben kann für im öffentlichen Interesse liegende Forschung angenommen werden, dass bei Social-Media-Daten, die »über die Online-Schnittstelle [der Plattfomen] öffentlich zugänglich sind«, keine »vernünftigen Erwartungen« (*reasonable expectations*)[44] an den Schutz der Privatsphäre vorliegen.[45] Bei Inhalten, die in vollständig öffentlichen Bereichen zirkulieren, d. h. auf den Nutzungsoberflächen der Plattform, die allen Nutzer:innen (oder potenziell auch Personen ohne registriertes Konto) zur Verfügung stehen, kann davon ausgegangen werden, dass die Nutzer:innen keine »vernünftigen Erwartungen« in Bezug auf die Privatsphäre haben.

Das Gesetz über digitale Dienste der EU (*DSA*) schreibt vor, dass Plattformen zugelassenen Forscher:innen »in Echtzeit Zugang zu öffentlich zugänglichen Daten« gewähren müssen, die »aggregierte Interaktionen mit Inhalten von öffentlichen Seiten, öffentlichen Gruppen oder Persönlichkeiten des öffentlichen Lebens, einschließlich Daten zu Wahrnehmung und Interaktion, wie z. B. die Anzahl der Reaktionen, Teilungen und Kommentare« umfassen können. Diese Art des Datenzugangs wird auch als *CrowdTangle*-Klausel bezeichnet. Mathias Vermeulen von *AWO Agency* stellt fest, dass es »für Unternehmen und Forscher:innen wahrscheinlich unzweckmäßig wäre, ein von dieser Klausel deutlich abweichendes Verfahren anzuwenden«.[46]

Parallel dazu sieht der von der EU 2022 gestärkte Verhaltenskodex zur Bekämpfung von Desinformation, der unter anderem von Google, Twitter, TikTok, Meta, Microsoft, Twitch und Vimeo unterzeichnet wurde, einen stabilen Zugang zu »kontinuierlichen, Echtzeit- oder echtzeitnahen, durchsuchbaren und nicht-personenbezogenen Daten und anonymisierten, aggregierten oder offenkundig öffentlichen Daten zu Forschungszwecken« vor, »wo immer dies sicher und praktikabel ist«. Dabei wird darauf hingewiesen, dass »offenkundig öffentliche Daten« auch »Konten von Personen des öffentlichen Lebens, wie beispielsweise von gewählten Vertreter:innen, Nachrichtenagenturen und Regierungskonten« umfassen können.[47]

In ähnlicher Weise beschreibt das *New York University (NYU)* Projekt *Cybersecurity for Democracy* solche Daten als »vernünftigerweise öffentliche Inhalte« (*reasonably public content*) und zählt dazu einschließlich Folgendes:

- Inhalte mit »hohem Engagement« (high engagement), wie z. B.:
  öffentliche Beiträge, die ein gewisses Maß an Viralität erreichen; öffentliche Beiträge in den größten öffentlichen Online-Foren, wie dem Subreddit *r/wallstreetbets*; öffentliche Inhalte von Konten mit einem sehr großen Zielpublikum, wie beispielsweise solche, die von sogenannten Influencer:innen veröffentlicht werden,
- öffentliche Inhalte von Regierungsstellen und Amtsträger:innen sowie von offiziellen Anwärter:innen auf ein Amt, unabhängig von ihrer Bekanntheit.[48]

Die im Kodex verwendete Formulierung »offensichtlich öffentlich gemachte Daten« stammt zwar aus der Datenschutzgrundverordnung (DSGVO). Dennoch bleibt unklar, wie die Unterzeichner des Kodex diesen Wortlaut in Bezug auf ihre eigenen Dienste auslegen.[49] Darüber hinaus wird in dem Kodex darauf hingewiesen, dass der Zugang zu automatisierten Mitteln »einem Bewerbungsverfahren unterliegen sollte, das nicht übermäßig schwerfällig sein sollte«.[50]

Meta: CrowdTangle

CrowdTangle verfolgt ausschließlich öffentliche Inhalte, zu denen Interaktionen/Engagement (Gesamtzahl der Reaktionen, Kommentare und Shares) auf öffentlichen Instagram-Konten, Facebook-Seiten, öffentlichen Facebook-Gruppen und Subreddits auf Reddit gehören. *CrowdTangle* gibt nicht den Text der Kommentare selbst weiter, sondern nur die Anzahl der Kommentare, ohne dabei zu unterscheiden, ob der Kommentar als Reaktion auf den Beitrag oder als Reaktion auf einen Kommentar zu dem Beitrag erfolgte. Folgendes wird von *CrowdTangle* nicht nachverfolgt:

- Reichweite bzw. *reach* (Anzahl von Personen, die einen Beitrag mindestens einmal gesehen haben);
- Impressionen bzw. *impressions* (wie oft ein Beitrag gesehen wurde);
- Einnahmen;
- 1-minütige Videoaufrufe (wie oft ein Video mindestens eine Minute lang abgespielt wurde, wobei erneute Wiedergaben des Videos nicht berücksichtigt werden);
- *Link Clicks* (Anzahl der Klicks auf einen Link oder den Beitrag selbst);
- sämtliche demografischen Angaben (Alter, Geschlecht usw.) auf der Ebene des Beitrags oder der Seite;
- ob der Inhalt einem Faktencheck unterzogen wurde.[51]

Forscher:innen kritisieren regelmäßig diesen Mangel an aussagekräftigen Metriken.[52] 2021 löste Meta das Team auf, das für *CrowdTangle* zuständig war. Dutzende ehemalige Mitarbeiter:innen haben entweder ihre Stelle im Unternehmen verloren oder neue Aufgaben in anderen Bereichen übernommen.[53] Ab Januar 2022 akzeptierte *CrowdTangle* keine neuen Nutzer:innen mehr und begründete dies mit »personellen Engpässen«, die seitdem nicht behoben wurden. Forscher:innen, die weiterhin auf die *API* zugreifen können, berichteten, dass diese seit 16 Monaten nicht mehr aktualisiert worden ist.[54] Stattdessen verlegte sich Meta zunehmend auf selektive Offenlegungen und veröffentlichte vierteljährlich einen Bericht unter dem Titel *Widely Viewed Content*. Dieser soll zeigen, welche Inhalte auf Facebook konsumiert wurden, und enthält Daten zur Anzahl der Aufrufe (*views*) und den Betrachtenden (*viewers*) von Inhalten, die im Feed in den USA[55] erscheinen. Da die berichteten Daten auf der Metrik ›Reichweite‹ beruhen, können sie von externen Forscher:innen nicht überprüft werden.

Im Zusammenhang mit dem Datenzugang für im öffentlichen Interesse liegenden Forschungszwecke sollte insofern die Existenz von Grauzonen anerkannt werden, als dass Inhalte nicht immer eindeutig in die Kategorie der »öffentlich zugänglichen Daten« oder der »nicht-öffentlichen Daten« eingeordnet werden können. So benutzt beispielsweise das *Center for Democracy & Technology* (*CDT*) den Begriff halböffentlich (*semi-public*) zur Bezeichnung von Daten, die nicht in dem Sinne öffentlich sind, als dass sie allen Nutzer:innen eines Dienstes zur Verfügung gestellt werden, die aber auch nicht ausschließlich nur an eine bestimmte Person oder eine sehr kleine Anzahl von Nutzer:innen gesendet werden.[56] Unter diese Kategorie fallen beispielsweise Discord-Kanäle, geschlossene Facebook-Gruppen, private Telegram-Kanäle, für die eine Einladungen erforderlich ist, Slack-Kanäle oder große WhatsApp-Gruppen. So leuchtet es beispielsweise ein, dass Inhalte, die in einer geschlossenen Gruppe mit Millionen von Mitgliedern veröffentlicht werden, zwar für einen großen Teil der Öffentlichkeit zugänglich sind, aber nicht als vollständig öffentlich gelten können.

Darüber hinaus sollten die Regelungen für den Datenzugang berücksichtigen, dass öffentlich zugängliche Daten *theoretisch* zu unrechtmäßigen Anwendungsfällen führen können, die in die Privatsphäre der Nutzer:innen eingreifen, wenn sie nicht auf eine im öffentlichen Interesse liegende Forschung beschränkt sind. Die Überwachung von Nutzern:innen durch die Strafverfolgungsbehörden und andere staatlichen Stellen, insbesondere in Situationen, in denen eine solche Überwachung nicht angemessen oder gerechtfertigt ist, könnte dazu führen, dass der Zugriff auf *APIs* zu unrechtmäßigen Zwecken erfolgt.[57]

Schließlich können auch einige der von den Plattformen generierten nicht-öffentlichen Daten für die im öffentlichen Interesse liegende Forschung erforderlich sein – so zum Beispiel Verlaufsdaten über das Verhalten von extremistischen Akteur:innen. Die Anträge auf Datenzugriff auf nicht-öffentliche Daten müssten im Rahmen von Zulassungs- bzw. Akkreditierungsmechanismen gesondert bewertet werden, da ein solcher Zugriff zweifellos das Risiko birgt, in die Privatsphäre der Nutzer:innen einzudringen, Geschäftsgeheimnisse oder von den Plattformen verwendete Sicherheitsmaßnahmen offenzulegen.

Empfehlungen:

- **Unternehmen und politische Entscheidungsträger:innen sollten sicherstellen, dass die Datenzugangsregelungen einen differenzierten und nuancierten Ansatz zum Schutz der Privatsphäre der Nutzer:innen beinhalten.** Von Nutzer:innen generierte Inhalte, die keine »vernünftigen Erwartungen« in Bezug auf den Datenschutz begründen, wie beispielsweise Inhalte, die auf öffentlichen Seiten, in öffentlichen Gruppen oder von Persönlichkeiten des öffentlichen Lebens gepostet werden, sollten über einen zulassungsbeschränkten *API*-Zugriff verfügbar gemacht werden. Dabei sollte auch auf die Metriken Reichweite, Impressionen und Engagement zugegriffen werden können. Bestimmte Arten der von Plattformen kuratierten Daten könnten in einem maschinenlesbaren Format anhand eines Verzeichnisses zugänglich gemacht werden, das die Entscheidungen zur Inhaltsmoderation archiviert. Andere Arten der von Plattformen kuratierten Daten, die sich darauf beziehen, wie Algorithmen Inhalte einstufen (z. B. Herabstufungspraktiken), sowie Daten zur Entscheidungsfindung der Plattformen müssten wahrscheinlich auf anderem Wege beschafft werden (z. B. durch Befragung von Mitarbeiter:innen).

- **Unternehmen sollten eine umfassende öffentliche Dokumentation über berechtigte Anwendungsfälle und Forschungsanforderungen für den Zugriff auf *API*-Endpunkte bereitstellen.** Dabei sollte eindeutig angegeben werden, welchen Zugriff Forscher:innen über die *API* erhalten können und welche Arten von Anwendungsfällen zulässig sind.

- **Aufsichtsbehörden und Forscher:innen sollten ergründen, warum Unternehmen die Abfrage historischer Daten oder das Datenvolumen begrenzen (z. B. nur die öffentlichen Posts der letzten sieben Tage oder nur 0,3 Prozent aller Tweets pro Monat).** Um beurteilen zu können, ob berechtigte Bedenken hinsichtlich der Kosten oder der Privatsphäre der Nutzer:innen diese Einschränkungen rechtfertigen, erfordern derartige Betrachtungen einschlägiges Fachwissen. Aufsichtsbehörden sollten die Unternehmen um Klarstellung dieser einschränkenden Maßnahmen bitten und sie gegebenenfalls beanstanden können, wenn diese die Forschung im öffentlichen Interesse beeinträchtigen.

Über Crowdsourcing und Datenspenden zugängliche Daten

Forscher:innen nutzen neben dem Zugriff über *APIs* und die Transparenzberichterstattung häufig auch unabhängige Möglichkeiten, um Plattformdaten zu beschaffen. Dabei muss nicht notwendigerweise eine Zustimmung des Dienstanbieters vorliegen. Bei der Bereitstellung von Daten über Datenspenden und Crowdsourcing installieren Teilnehmer:innen ein Plugin, mit dem sie ihre Daten an ein bestimmtes Forschungsprojekt weitergeben, das eine bestimmte Plattform untersucht. Wichtig ist, dass die Nutzer:innen der Verwendung ihrer Daten zu diesem speziellen Zweck zustimmen. Im Erwägungsgrund 33 der DSGVO wird gefordert, dass die betroffenen Personen – also die Nutzer:innen – »Gelegenheit erhalten sollten, ihre Einwilligung nur für bestimme Forschungsbereiche oder Teile von Forschungsprojekten in dem vom verfolgten Zweck zugelassenen Maße zu erteilen«. Im Gegensatz zur Verwendung von sogenannten Sockenpuppen-Accounts, die versuchen, die Erfahrungen von Nutzer:innen mit bestimmten Eigenschaften oder Interessen zu simulieren, können Datenspenden Einblicke in das reale Verhalten der Nutzer:innen geben.

Im Juli 2021 veröffentlichte Mozilla die bisher größte auf Crowdsourcing basierende Untersuchung des Empfehlungssystems von YouTube.[58] Der Datensatz wurde von 37.380 Teilnehmer:innen aus 190 Ländern gespeist, die die Browsererweiterung *RegretsReporter* für Firefox und Chrome installiert hatten. Mozilla gab an, dass dieser »personengestützte Ansatz« die realen Erfahrungen der YouTube-Nutzer:innen einfangen konnte und einen gewissen Einblick in den Algorithmus ermöglichte, obwohl YouTube nicht bereit war, den Forscher:innen Daten zur Verfügung zu stellen. Dabei verzichtete Mozilla absichtlich auf eine strikte Definition für ein *YouTube Regret*, um den Menschen die Möglichkeit zu geben, das gesamte Spektrum negativer Erfahrungen abzubilden, die sie auf YouTube machen. Mithilfe des Dienstes zur Geolokalisierung *GeoIP* konnten die Forscher:innen feststellen, von welchem Land aus die Teilnehmer:innen auf YouTube zugriffen, und somit auch geografische und sprachliche Besonderheiten einbeziehen. Mozilla erkannte jedoch auch die methodischen Limitationen dieses Vorgehens an, darunter die Auswahlverzerrung (bei den Teilnehmer:innen handelt es sich um eine spezielle Gruppe von Nutzern:innen), die Meldeverzerrung (es kann viele Faktoren geben, die beeinflussen, ob die Teilnehmer:innen ein bestimmtes Video melden) sowie den Beobachtungscharakter der Methode. Letzteres bedeutet, dass die Forscher:innen nicht in der Lage sind, mit Sicherheit zu folgern, warum etwas passiert. So bleibt den Forscher:innen beispielsweise verborgen, warum YouTube den Teilnehmer:innen ein bestimmtes Video empfohlen hat.

Im September 2022 veröffentlichte Mozilla eine weitere Studie, in welcher die Feedback-Werkzeuge von YouTube untersucht wurden. Dabei wurde anhand von Crowdsourcing-Daten von 22.838 Teilnehmer:innen analysiert, was im Laufe der Zeit mit den Videoempfehlungen der Nutzer:innen geschah, nachdem sie eines der Werkzeuge (z. B. den Dislike-Button) verwendet hatten.[59] Auch diese Studie wurde mithilfe freiwilliger Teilnehmer:innen durchgeführt, welche wiederum zu diesem Zweck die oben erwähnte Web-Erweiterung installiert hatten. Die mit der Erweiterung erfassten Daten wurden über die Firefox-Telemetrie an Mozilla-Server gesendet. Unter anderem wurde aufgezeichnet, wann (Zeitstempel) und für welches Video (Video-ID) im Feed von der Option »Keine Videos von diesem Kanal empfehlen« Gebrauch gemacht wurde. Außerdem wurden alle von YouTube ausgespielten Empfehlungen, einschließlich Zeitstempel, Video-ID und der Art der Empfehlung, sowie alle Interaktionen mit den nativen Steuerungsfunktionen für Nutzer:innen aufgezeichnet. Die Studie ergab, dass die Teilnehmer:innen das Gefühl hatten, die von YouTube vorgesehenen Möglichkeiten zur nutzerseitigen Steuerung würden die Empfehlungen überhaupt nicht beeinflussen. Stattdessen versuchten die Teilnehmer:innen, ihre Empfehlungen durch Ausprobieren zu kontrollieren – mit begrenztem Erfolg. Diese Methodik erforderte zudem beträchtliche technische, finanzielle und personelle Ressourcen, wobei ein großer Teil des Aufwands auf die Aufklärungsarbeit im Zusammenhang mit der Nutzung der Web-Erweiterung und die Verpflichtung der Teilnehmer:innen zur Einholung einer Einwilligungserklärung entfiel. Allein schon deshalb ist es unwahrscheinlich, dass diese Art von Crowdsourcing auch für kleinere Forschungseinrichtungen anwendbar ist.

Facebook hat in der Vergangenheit den Einsatz von Crowdsourcing-Methoden behindert. Insbesondere der Einsatz der von *NYU Cybersecurity for Democracy* entwickelten Webbrowser-Erweiterung *Ad Observer,* die die Werbeanzeigen, die den Nutzer:innen auf Facebook

und YouTube angezeigt werden, aufzeichnet und in eine öffentliche Datenbank kopiert, war dem Unternehmen ein Dorn im Auge. Die Erweiterung sollte folgende Daten erfassen: den Namen des Werbetreibenden und den Hinweistext (*disclosure string),* den Text, das Bild und den Link der Anzeige, die von Facebook bereitgestellten Informationen zur Zielgruppe der Anzeige, wann die Anzeige gezeigt wurde, und die Browsersprache. Personenbezogene Daten wurden dagegen nicht erfasst. Das Tool zielte darauf ab, mehr Transparenz in die politische Werbung zu bringen, die bei Präsidentschaftswahlen von großer Bedeutung ist. Meta hat sich jedoch entschieden, die Konten der beiden an der NYU tätigen Wissenschaftler:innen Laura Edelson und Damon McCoy zu sperren und ihnen den Zugriff auf Daten der *Ad Library* und der *CrowdTangle-API* zu verwehren.[60] Das Unternehmen berief sich auf Bedenken hinsichtlich des Datenschutzes der Nutzer:innen, die sich aus dem Vergleich mit der *Federal Trade Commission* (*FTC*) nach dem Skandal um *Cambridge Analytica* und der entsprechenden Klage ergeben hätten. Die *FTC* stellte jedoch klar, dass der Vergleich Meta nicht dabei im Weg stand, für derartige Forschungsvorhaben Zugriff auf Daten zu gewähren. Mozilla erklärte außerdem, dass auch die Bedenken in Bezug auf den Datenschutz nur vorgeschoben seien. Mozilla überprüfte sowohl den Code der Erweiterung als auch den Einwilligungsprozess, um sicherzustellen, dass die Nutzer:innen genau verstehen, was sie installieren. Mozilla kam zu dem Schluss, dass die Vereitelung des Forschungsprojekts unter Berufung auf die Datenschutzbestimmungen von Meta nicht gerechtfertigt war, da die Erweiterung keine persönlichen Daten oder Informationen über die Facebook-Freunde der Teilnehmer:innen sammelte.[61]

USA: *Platform Accountability and Transparency Act (PATA)*

Der *PATA*, der von den US-Senator:innen Chris Coons (D-DE), Rob Portman (R-OH), Amy Klobuchar (D-MN) und Bill Cassidy (R-LA) im 117. Kongress (2021-2022) eingebracht wurde, soll die Transparenz der Social-Media-Unternehmen erhöhen. Das Gesetz würde Forscher:innen an Universitäten und von gemeinnützigen Organisationen in den USA Zugriff auf die Daten der größten Social-Media-Unternehmen gewähren und öffentliche Transparenz in Bezug auf die »am häufigsten geteilten Beiträge, Werbeanzeigen, Inhaltsmoderationspraktiken und Empfehlungsalgorithmen« schaffen.

Der Gesetzentwurf sieht außerdem einen gewissen Rechtsschutz für Forscher:innen vor, die Daten von Social-Media-Plattformen »durch eine anerkannte digitale Untersuchungsmethode« erfassen und dabei »angemessene Maßnahmen« zum Schutz der Privatsphäre der Nutzer:innen ergreifen.[62] Zu den zulässigen Methoden (*covered methods*) zählt »die Erhebung von Daten, die von Nutzer:innen einschließlich mittels Browsererweiterung oder ein Plugin gespendet werden, wenn die Datenspende im Zusammenhang mit dem Projekt und mit ausdrücklicher Zustimmung der Nutzer:innen erfolgt«. Zu den Daten, deren Erhebung demnach zulässig wäre, gehören »öffentlich verfügbare Informationen, Informationen über Anzeigen, einschließlich des Namens des Werbetreibenden und des Hinweistextes, sowie Informationen, die die Plattform den Nutzer:innen in Bezug darauf zur Verfügung stellt, wie die Zielgruppe einer Anzeige ermittelt wurde«, sowie jede andere Kategorie von Informationen, die »die Privatsphäre der Nutzer:innen nicht unangemessen beeinträchtigen würden«.

Zu den Vorkehrungen zum Schutz der Privatsphäre der Nutzer:innen gehören Maßnahmen zur »Vermeidung der Sammlung und Aufbewahrung nicht-öffentlicher Informationen, mit denen Nutzer:innen ohne ihre Zustimmung leicht identifiziert werden können« und zur »Verhinderung von Diebstahl und versehentlicher Offenlegung aller erfassten Daten«.

Empfehlungen:

- **Politische Entscheidungsträger:innen sollten Forscher:innen rechtlich schützen, damit diese Plattformen unter Einhaltung von Datenschutzvorkehrungen untersuchen können.** Ein rechtlicher Schutzraum sollte Forscher:innen von zivilrechtlichen Haftungsansprüchen begründet freistellen. Wenn Forscher:innen diesen rechtlichen Schutz bekämen, sollte es den Plattformen untersagt werden, deren Konten zu sperren oder technische Maßnahmen zu ergreifen, um deren Zugriff auf Daten zu blockieren.[63]

- **Unternehmen sollten in den Nutzungsbedingungen ihrer Plattformen freiwillige Ausnahmeregelungen vorsehen, um Untersuchungen unter Verwendung von Methoden wie dem Crowdsourcing von Daten zu ermöglichen. Eine Voraussetzung hierfür ist, dass die Forscher:innen Datenschutzbestimmungen einhalten – einschließlich der Einholung einer aufgeklärten Zustimmung der Teilnehmer:innen.** Mozilla erklärt zum Beispiel ausdrücklich, dass Personen, die sich in gutem Glauben um die Einhaltung seines Bug-Bounty-Programms bemühen, keine Drohungen oder rechtlichen Schritte seitens des Unternehmens zu befürchten haben. Das Programm fördert ausdrücklich die Forschung, mit der Sicherheitslücken in Produkten von Mozilla gefunden werden sollen, wobei das Unternehmen sogar Prämien für gefundene Fehler zahlt. Dabei liefert Mozilla zudem ein Beispiel für gute Praktiken, indem es den Rechtsschutz für die daran beteiligten Forscher:innen sicherstellt und zusichert, dass es Forscher:innen weder nach dem Gesetz noch nach den geltenden Nutzungsbedingungen und der *Acceptable Use Policy* für ihre Forschungstätigkeit im Rahmen des *Bug-Bounty*-Programms verklagen wird.[64]

Aufbau einer Infrastruktur für den Datenzugang: Auf dem Weg zur internationalen politischen Harmonisierung

Angesichts der inhärenten globalen Dimension des Internets und von Social-Media-Plattformen ist es naheliegend, dass liberal-demokratische Regierungen ihre Absichten in Bezug auf Transparenzpflichten und Datenzugangsregelungen aufeinander abstimmen. Zur Vereinheitlichung und Zusammenführung der Ansätze sind dabei nicht notwendigerweise neue Gesetze erforderlich, deren Verabschiedung oft mit erheblichen politischen Hürden verbunden ist.

Einen vielversprechenden Ansatz für die Harmonisierung der Internet-Governance zwischen liberalen Demokratien mit unterschiedlichen Rechtssystemen, Regulierungsbedarfen und gesellschaftlichen Normen bietet ein von Susan Ness und Chris Riley unter der Bezeichnung »Modularität« (*modularity*) vorgeschlagener Multi-Stakeholder-Prozess zur Ko-Regulierung. Die dabei geschaffenen Module werden unter Beteiligung verschiedener Stakeholder zur grenzübergreifenden Bearbeitung gemeinsamer Aufgabenstellungen genutzt. Zu diesen gemeinsamen Aufgaben können beispielsweise die Zulassung von Forscher:innen für den Zugang zu Plattformdaten und die Genehmigung ihrer Forschungsvorschläge zählen. Weiter sieht der Vorschlag vor, dass eine internationale Expert:innengruppe, in der unterschiedliche Stakeholder vertreten sind, Standards und Protokolle für den Zugang zu Plattformdaten erstellt und ein unabhängiges Gremium für die Verwaltung des Zulassungssystems bildet. Die einzelnen Staaten würden formell oder informell anerkennen, dass das Modul die Anforderungen an die Zulassung von Forscher:innen in ihrem jeweiligen Rechtsrahmen erfüllt, und weiterhin für die Durchsetzung verantwortlich bleiben. Auslaufklauseln (*sunset provisions*) würden bewirken, dass das Modul auf dem neuesten Stand bleibt und für den jeweiligen Zweck geeignet ist.

Durch grenzübergreifende Module dieser Art können die begrenzten Ressourcen der Aufsichtsorgane geschont werden, da diese zur Erfüllung gleicher Aufgaben sonst jeweils eigene Systeme benötigen würden. Die Konformität von Plattformen ließe sich durch die mit den Modulen verbundene Standardisierung der Prozesse und Regeln sogar erhöhen, weil weniger Unsicherheit in Bezug auf deren Anwendung zu erwarten wäre. Darüber hinaus trägt die grenzübergreifende Beteiligung an der Wahrnehmung gemeinsamer Aufgaben zur Stabilisierung und Stärkung der Demokratien bei.

Europäische Union: Gestärkter Kodex zur Bekämpfung von Desinformation von 2022

Die auf EU-Ebene entstehende Infrastruktur für den Datenzugang umfasst neben den Verpflichtungen im Rahmen des Gesetzes über digitale Dienste (*Digital Services Act, DSA*) und den Verpflichtungen der Unterzeichnenden des 2022 gestärkten Kodex zur Bekämpfung von Desinformation (*The 2022 Code of Practice on Disinformation, CoPD*) auch den Entwurf der Europäischen Beobachtungsstelle für digitale Medien (*European Digital Media Observatory, EDMO*) für einen Verhaltenskodex, der regeln soll, wie Plattformen Daten mit unabhängigen Forscher:innen teilen und gleichzeitig die Rechte der Nutzer:innen schützen können.

Über die Festlegungen des *DSA* hinaus haben sich unterzeichnende Tech-Unternehmen wie Google, Twitter, Microsoft, Meta und TikTok zur Bereitstellung von Daten verpflichtet, mit denen die Forschung über Desinformation im Rahmen des *CoPD* ermöglicht werden soll. Die Datenzugangsregelung nach dem *CoPD* unterscheidet sich dem Zweck nach vom *DSA*, da der Zugang zu jedem beliebigen Forschungszweck im Zusammenhang mit dem Thema »Desinformation«[65] gewährt werden kann und nicht auf die Bewertung und Prüfung der Maßnahmen der Plattformen zur Risikobewertung und -minderung beschränkt ist.

Im Rahmen ihrer Verpflichtungen haben die unterzeichnenden Unternehmen im Februar 2023 die Website *Transparency Centre* eingerichtet. Die Website soll die Verpflichtungen und Maßnahmen aus dem Kodex in einer leicht verständlichen und durchsuchbaren Form enthalten. Die Website enthält auch ein Archiv der Berichte der unterzeichnenden Unternehmen in den Formaten PDF, CSV und JSON. Diese Berichte umfassen regelmäßige qualitative Elemente der Berichterstattung sowie quantitative »*Service Level Indicators*«. Darüber hinaus verpflichteten sich die Unternehmen mit einer Task Force an der Entwicklung von »*Structural Indicators*« zu arbeiten, um die Wirksamkeit des Kodex hinsichtlich der Eindämmung der Verbreitung von Online-Desinformation auf umfassende Weise zu bewerten. Die unterzeichnenden Unternehmen haben für die Entwicklung und Umsetzung dieser »*Structural Indicators*« eine Arbeitsgruppe eingerichtet, die sich aus Expert:innen zusammensetzt, darunter Vertreter:innen von *EDMO* sowie der Gruppe der europäischen Regulierungsbehörden für audiovisuelle Mediendienste (*ERGA*).[66]

Die Unterzeichner des *CoPD* haben sich insbesondere dazu verpflichtet, »eine unabhängige, dritte Stelle aufzubauen, zu finanzieren und mit ihr zu kooperieren, die für die Zulassung von Forscher:innen und Forschungsvorschlägen zuständig sein kann«. Eine solche Stelle könnte vermutlich die Aufgaben des im *DSA* vorgeschlagenen »unabhängigen Beratungsmechanismus zur Unterstützung der Datenweitergabe« an Forscher:innen und der von der *EDMO*-Arbeitsgruppe vorgeschlagenen »unabhängigen Vermittlungsstelle« zusammenführen.

Erwartungen an den Datenschutz

Ein datenschutzkonformer Datenzugang sollte die Erwartungen an den Datenschutz in den verschiedenen Rechtsordnungen widerspiegeln und die höchsten bestehenden Standards anstreben. Mit der Verabschiedung der DSGVO hat die EU die wohl strengste Datenschutzgesetzgebung der Welt geschaffen.[67] Seitdem läuft eine intensive Debatte über ihre Auswirkungen auf die Bereitstellung von Plattformdaten für im öffentlichen Interesse liegende Forschungszwecke.

2022 veröffentlichte die Arbeitsgruppe der Europäischen Beobachtungsstelle für digitale Medien (*EDMO*) zur Klärung der Anwendung der Datenschutzpflichten aus der DSGVO im Forschungskontext einen Entwurf für die gemäß Artikel 40 der DSGVO vorgesehenen Verhaltensregeln.[68] Die zwölf Mitglieder der aus Wissenschaftler:innen sowie aus Vertreter:innen der Zivilgesellschaft und der Industrie bestehenden Arbeitsgruppe trafen sich regelmäßig, um die rechtlichen, ethischen, technischen und wissenschaftlichen Möglichkeiten zur Gewährleistung des Datenzugangs zu besprechen.[69] Der Arbeitsgruppe gehörten auch Vertreter:innen von Meta, Twitter und Google an. Im Rahmen des Abschlussberichts der *EDMO* haben Meta und Twitter sogenannte *Concurring Opinions Letter*s eingereicht.[70]

Die Arbeitsgruppe der *EDMO* bestätigte insbesondere die Auffassung, dass die DSGVO die gesellschaftliche Bedeutung der Forschung bereits widerspiegelt, indem sie besondere Regelungen für die Datenverarbeitung zu Forschungszwecken vorsieht und rechtliche Rollen, Verantwortlichkeiten und Haftungen sowohl für Plattformen als auch für Forscher:innen festlegt. Insbesondere erleichtert die DSGVO die Verarbeitung personenbezogener Daten für Forschungszwecke durch eine »Vereinbarkeitsvermutung«, die in Artikel 5 (Absatz 1 b) verankert ist und besagt, dass die Verarbeitung personenbezogener Daten für »im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche oder historische Forschungszwecke nicht als unvereinbar mit den ursprünglichen Zwecken« der Datenverarbeitung angesehen wird.

Zwar wird der Begriff »Forschungszwecke« in der DSGVO selbst nicht ausdrücklich definiert, doch heißt es in Erwägungsgrund 159: »Die Verarbeitung personenbezogener Daten zu wissenschaftlichen Forschungszwecken im Sinne dieser Verordnung sollte weit ausgelegt werden und die Verarbeitung für beispielsweise die technologische Entwicklung und die Demonstration, die Grundlagenforschung, die angewandte Forschung und die privat finanzierte Forschung einschließen.«[71]

Der Europäische Datenschutzbeauftragte führte dazu aus, dass diese Vereinbarkeitsvermutung direkt im Zusammenhang mit der Anforderung zu sehen ist, angemessene technische und organisatorische Datenschutzvorkehrungen wie Pseudonymisierung und Zugangsbeschränkungen zu gewährleisten. Jede sekundäre, mit der DSGVO vereinbarte Verarbeitung der Daten muss somit allen anderen Regeln der DSGVO von der Datenminimierung über die Begrenzung der Aufbewahrung bis hin zur Gewährleistung der angemessenen Sicherheit entsprechen.[72] Der Entwurf für den Verhaltenskodex sieht vor, dass die Sicherheitsmaßnahmen der Art und dem Zweck der Verarbeitung sowie den Risiken für die Rechte und Freiheiten des Einzelnen angemessen sein müssen. Typische Datensicherheitsrisiken, die von der DSGVO erfasst werden, betreffen beispielsweise die Geheimhaltung (unbefugte Offenlegung von oder unbefugter Zugang zu personenbezogenen Daten), die Integrität (unrechtmäßige oder unbeabsichtigte Änderung) und die Verfügbarkeit (unbeabsichtigte oder unrechtmäßige Zerstörung). Für den Fall, dass ein Forschungsvorhaben zur Erfüllung seines Zwecks personenbezogene Daten erfordert, sind von den Forscher:innen nach dem Kodex Maßnahmen wie Anonymisierung oder Pseudonymisierung der Daten, einschließlich geeigneter Schritte zur Verhinderung einer erneuten Identifizierung der betroffenen Personen, zu ergreifen.[73]

Empfehlungen:

- **Politische Entscheidungsträger:innen in EU- und Nicht-EU-Ländern sollten die bestehenden Datenschutzverpflichtungen der DSGVO – insbesondere die spezifischen Ausnahmen in Bezug auf die Verarbeitung zu im öffentlichen Interesse liegenden Archivzwecken und zu wissenschaftlichen Forschungszwecken – als internationalen Standard für Datenschutzvorkehrungen nutzen.** In diesem Zusammenhang könnte der von der *EDMO* vorgeschlagene Verhaltenskodex als Grundlage für die grenzübergreifende Zusammenarbeit bei datenschutzkonformen Datenzugangsregelungen sowohl innerhalb als auch außerhalb der EU dienen.

Zugelassene Forscher:innen

Der automatisierte und strukturierte Datenzugang über *APIs* auf öffentliche (sowie gegebenenfalls halböffentliche und nichtöffentliche) Daten sollte nicht nur die Datenverarbeitung durch Forscher:innen und Plattformen, sondern auch die potenziellen Risiken eines unbefugten Zugriffs (oder einer anderen Verarbeitung) berücksichtigen. Zugelassenen Forscher:innen wäre es somit verboten, Daten und Informationen für kommerzielle Zwecke zu nutzen oder diese Daten an unbefugte Dritte weiterzugeben.

Der DSA enthält keine konkreten Vorgaben bezüglich der Verfahren für die Zulassung von Forscher:innen und die Gewährung des Datenzugangs, die von der Kommission in delegierten Rechtsakten zu klären sind. Allerdings listet die Verordnung mehrere Bedingungen auf, die Forscher:innen für die Freigabe durch den Koordinator für digitale Dienste am Niederlassungsort (*Digital Services Coordinator of Establishment*) erfüllen müssen, wobei es sich hierbei um die Aufsichtsbehörde des Landes handelt, in dem ein Unternehmen seinen europäischen Hauptsitz hat. Aktuell wäre dies in vielen Fällen die irische Aufsichtsbehörde.[74] Dementsprechend erfüllen Forscher:innen die Zulassungsvoraussetzungen, wenn sie »einer Forschungseinrichtung angeschlossen sind, die wissenschaftliche Forschung mit dem vorrangigen Ziel betreiben, ihren Auftrag im öffentlichen Interesse zu unterstützen«.

In ähnlicher Weise bekräftigt der von der *EDMO* vorgeschlagene Verhaltenskodex, dass »qualifizierte Forschung« auf der Grundlage der DSGVO auf den »Aufbau des kollektiven Wissens der Gesellschaft« abzielen und von einer »Einrichtung durchgeführt werden muss, zu deren Hauptzielen die Forschungsarbeit auf nicht gewinnorientierter Basis zählt«. Mathias Vermeulen von *AWO Agency* vermutet, dass dies »wahrscheinlich auch für Forschungsgruppen gelten würde, an denen Forscher:innen und Journalist:innen aus Nicht-EU-Ländern beteiligt sind, solange unter den Forscher:innen ein europäischer Hauptantragsteller ist«.[75] Die Forscher:innen müssten außerdem ihre Mittelherkunft offenlegen und ihre Unabhängigkeit von kommerziellen Interessen nachweisen. In einem Zulassungsverfahren müssten Forscher:innen Folgendes tun:

- geeignete technische und organisatorische Maßnahmen zur Wahrung der Datensicherheit und der Vertraulichkeitsanforderungen beschreiben;
- begründen, warum die Daten für ihren Forschungszweck notwendig sind und wie die Forschung zum Verständnis der »systemischen Risiken in der Union« oder der »Angemessenheit, der Wirksamkeit und der Auswirkungen der Risikominderungsmaßnahmen« beitragen würde;
- sich verpflichten, ihre Forschungsergebnisse öffentlich und kostenlos zur Verfügung zu stellen;
- angeben, welches Datenzugangsformat sie idealerweise bevorzugen und zu welchem Datum sie Zugang zu den Daten benötigen.

Im *DSA* ist nicht festgelegt, ob die Zulassung von Forscher:innen bereits vorliegen muss, bevor ein Antrag auf Datenzugang gestellt werden kann, oder ob beide Prozesse gleichzeitig stattfinden können. Die Zulassungsmechanismen könnten auf einer projektbezogenen Basis beruhen, sodass Forscher:innen entsprechend dem dazugehörigen Antrag auf Datenzugang im spezifischen Einzelfall zugelassen werden. Ein solches Vorgehen würde den Schwerpunkt weniger darauflegen, wer die Daten anfordert, sondern darauf, ob das jeweilige Forschungsprojekt als solches die Voraussetzungen erfüllt.

Empfehlungen:

- **Politische Entscheidungsträger:innen und Aufsichtsbehörden sollten sicherstellen, dass die Mechanismen für die Zulassung von Forscher:innen Gesetzeslücken für den unbefugten Zugriff auf Daten durch Unternehmen, Regierungs- oder Strafverfolgungsbehörden schließen und gleichzeitig die unabhängige Forschung im öffentlichen Interesse stärken.** Auch wenn die Zugehörigkeit (*affiliation*) zu einer akademischen Einrichtung dabei als Gatekeeper-Funktion dienen kann, sollten auch Forscher:innen ohne akademischen Hintergrund zugelassen werden. Klare Begriffsbestimmungen für die Bedeutung von Formulierungen wie »einer Forschungsrichtung angeschlossen/zugehörig« (*affiliated*) oder »mit einer Forschungseinrichtung assoziiert« (*associated*) sollten für Klarheit bei der rechtlichen Auslegung und eine breite Anwendbarkeit auf die im öffentlichen Interesse liegende Forschung sorgen. Dies sollte auch für Forscher:innen gelten, die ihren Sitz außerhalb der EU haben, wenn sie die Einhaltung der Datenschutzvorkehrungen nachweisen können.

- **Politische Entscheidungsträger:innen und Aufsichtsbehörden sollten die grenzübergreifende Anwendung der eingerichteten Zulassungsmechanismen für Forscher:innen eindeutig regeln.** Die internationale Zusammenarbeit zwischen liberal-demokratischen Staaten könnte sich neben den im Entwurf für den Verhaltenskodex der *EDMO* enthaltenen Vorschlägen auf die Vereinheitlichung und Integration der Zulassungsverfahren konzentrieren.

- **Politische Entscheidungsträger:innen, Aufsichtsbehörden und Unternehmen sollten anerkennen, dass Zeit ein wichtiger Faktor bei Forschungsprojekten sein kann, und diese auf den rechtzeitigen Zugriff auf Daten angewiesen sind. Dies trifft insbesondere in Krisensituation zu, die eine Bedrohung für die öffentliche Sicherheit oder Gesundheit darstellen.** Die Akkreditierungsmechanismen für die Zulassung von Forscher:innen sollten eine effiziente und angemessene Bearbeitung von Anträgen auf Datenzugang sicherstellen, wann immer dies möglich ist. Agil ausgestaltete Zulassungsverfahren könnten auf den im *DSA* vorgesehenen Krisenreaktionsmechanismus abgestimmt werden, der die Europäische Kommission ermächtigt, in Krisensituationen zusätzliche Ad-hoc-Risikobewertungen von sehr großen Online-Plattformen (*VLOPs*) und sehr großen Online-Suchmaschinen (*VLOSEs*) zu fordern. Die Gewährleistung zügiger Zulassungen und eines rechtzeitigen Zugangs zu Daten könnte auch die unabhängige Kontrolle der Wirksamkeit und Verhältnismäßigkeit aller im Rahmen der Krisenreaktionsmechanismen getroffenen Maßnahmen stärken.[76]

- **Politische Entscheidungsträger:innen und Aufsichtsbehörden sollten Zulassungsverfahren nicht nur wegen der Einhaltung von Vorschriftenin Erwägung ziehen, sondern auch aus Gründen einer im öffentlichen Interesse liegenden Forschung.** Da neben der Untersuchung von Desinformation und »systemischen Risiken« auch andere Anlässe für die Anforderung von Plattformdaten durch Forscher:innen vorstellbar sind, sollten Zulassungen auch für im öffentlichen Interesse liegende Forschungsprojekte offenstehen, die darauf abzielen, die Auswirkungen sozialer Medien auf die Gesellschaft als Ganzes zu verstehen.

Unabhängige Vermittlungsstelle: Die Beziehungen zwischen Aufsichtsbehörden, Forscher:innen und Plattformen

Im Artikel 41 der DSGVO ist ausdrücklich vorgesehen, dass »die Überwachung der Einhaltung von Verhaltensregeln« durch eine dafür eingerichtete Stelle durchgeführt werden kann, die über »geeignetes Fachwissen« hinsichtlich der Verhaltensregeln für den Datenzugang durch Forscher:innen verfügen muss. In Bezug auf den *Status quo* stellte die Arbeitsgruppe der *EDMO* jedoch fest, dass eine solche unabhängige Vermittlungsstelle (*independent intermediary body*), die die Überwachung und gegebenenfalls auch die Umsetzung der in den Verhaltensregeln (Kodex) vorgesehenen Prozesse unterstützen könnte, bisher fehlt. Damit ist eine entscheidende Schwachstelle noch nicht geschlossen worden.

Im Einzelnen empfiehlt die Arbeitsgruppe nachdrücklich die Einrichtung einer solchen Stelle, die (a) bescheinigt, dass die Forscher:innen qualifiziert und kompetent sind, um die Forschung durchzuführen, (b) überprüft, ob die Forschung als solche die Zulassungsvoraussetzungen erfüllt, und (c) diese Bescheinigungen den Plattformen und allen anderen relevanten Parteien zur Verfügung stellt.[77]

Zum einen könnte die Straffung der Prüfungs- und Zertifizierungsprozesse und deren Bündelung in einer unabhängigen Vermittlungsstelle die Belastung für kleinere, ressourcenschwache Universitäten und Forschungseinrichtungen verringern. Angesichts der großen Unterschiede bei den Ressourcen und Kapazitäten der staatlichen Aufsichtsbehörden in der EU stellt Mathias Vermeulen fest, dass eine zwischengeschaltete Stelle notwendig sein könnte, um geeignete Rahmenbedingungen, Fähigkeiten und Kenntnisse zu gewährleisten, damit die Vielfalt von Anträgen auf Datenzugang einschließlich der entsprechenden Forschungskonzepte und -methoden überhaupt bewertet werden kann.[78]

In ähnlicher Weise betont Julian Jaursch von der *Stiftung Neue Verantwortung (SNV)*, dass eine neue »Riege von Sachverständigen« in den staatlichen Institutionen benötigt wird. Dabei bezieht er sich auf die Aufsichtsbehörden, die im Rahmen des *DSA* die Rolle des Koordinators für digitale Dienste übernehmen werden. Jaursch unterstreicht die Notwendigkeit, erfahrene

Praktiker:innen und Akademiker:innen aus einer Vielzahl von Fachgebieten zu mobilisieren und gleichzeitig starke Verbindungen zur akademischen Welt und zur Zivilgesellschaft zu pflegen.[79] Letztendlich wird die Bewertung der Machbarkeit, Zweckmäßigkeit und Bedeutung von Anträgen auf Datenzugang aus den Kreisen der Forscher:innen umfassende methodische Kompetenzen und datenwissenschaftliche Kenntnisse erfordern.[80]

Eine unabhängige Vermittlungsstelle auf EU-Ebene könnte dabei helfen, eine Sachverständigengemeinschaft aufzubauen und gemeinsame Standards für die Überprüfung und Zertifizierung der Datensätze, Codebücher und technischen Systeme der Plattformen zu schaffen. Eine unabhängige Vermittlungsstelle könnte darüber hinaus auch Forscher:innen und Forschungseinrichtungen außerhalb der EU unterstützen. So könnte die Stelle beispielsweise durch die Koordinierung von Zulassungsverfahren für Datenzugangsanfragen zu einer weiteren internationalen Harmonisierung beitragen. Eine solche Koordinierung könnte den Austausch mit Aufsichtsbehörden außerhalb der EU umfassen, zum Beispiel aus Großbritannien, der Schweiz, Australien, Neuseeland, Kanada und den USA. Für transatlantische Initiativen könnten die politischen Entscheidungsträger:innen die Arbeitsgruppen des *EU-US Trade and Technology Councils* als Kooperationsforum nutzen.

Empfehlungen:

- **Um Interessenskonflikte zu vermeiden und eine demokratische Kontrolle zu gewährleisten, sollten die Aufsichtsbehörden sicherstellen, dass eine vermittelnde Stelle selbst bestimmte Transparenzstandards einhält.** Hierzu könnte neben einer transparenten Dokumentation von Besprechungen mit Branchenvertreter:innen und einem wirksamen Schutz von Whistleblowern auch die Festlegung von Karenzzeiten zählen, die verhindern, dass Personen, die zuvor für die unabhängige Vermittlungsstelle tätig waren, unmittelbar danach auf Positionen in Tech-Unternehmen wechseln dürfen. Die Vermittlungsstelle könnte Informationen darüber veröffentlichen, ob und warum ein Antrag auf Datenzugang gewährt oder abgelehnt wurde. Diese Informationen könnten auch Auskunft über die Anzahl der Anträge sowie allgemeine Informationen über die Projektvorschläge und die Arten der angeforderten Daten geben.
- **Die Aufsichtsbehörden sollten dafür sorgen, dass eine vermittelnde Stelle über ausreichendes wissenschaftliches Fachwissen und personelle Ressourcen verfügt, damit diese in der Lage ist, die Forschungsziele, die methodischen und ethischen Standards sowie die technischen und operativen Datenschutzvorkehrungen im Rahmen der Zulassungsverfahren zu beurteilen.** Es braucht ausreichende Ressourcen, um Bedenken, die zur Ablehnung von Anfragen durch die Plattformen führen, zu vermeiden oder vorzubeugen. In Anbetracht des erforderlichen Fachwissens und der benötigten Ressourcen könnte ein regelmäßiger Wissensaustausch zwischen den staatlichen Aufsichtsbehörden innerhalb und außerhalb der EU, die mit den gleichen Aufgaben betraut sind, Skalierbarkeit gewährleisten.
- **Politische Entscheidungsträger:innen, Aufsichtsbehörden und Forscher:innen sollten eine länderübergreifende Strategie für eine Vermittlungsstelle fördern.** Eine Vermittlungsstelle könnte – unter Berücksichtigung der Datenschutzregelungen der DSGVO –Verzeichnisse von öffentlichen Daten entwickeln und bereitstellen, die von Forscher:innen außerhalb der EU genutzt werden können. Diese Maßnahmen sollten der Transparenz der Forschungsgemeinschaft zugutekommen, indem sie dazu beitragen, wiederkehrende Arbeit zu vermeiden. Die Vermittlungsstelle könnte beispielsweise einen zentralen öffentlichen *Store* für Datenkataloge und Codebücher vorantreiben, in dem spezifiziert und erläutert wird, welche Arten von Social-Media-Daten verfügbar sind.

Fazit

Tech-Unternehmen verfügen über riesige Datenmengen, die von den Nutzer:innen generiert und von den Plattformen kuratiert werden. Die darin enthaltenen Informationen sind von enormem Wert für die im öffentlichen Interesse liegende Forschung, die auf ein besseres Verständnis komplexer politischer und gesellschaftlicher Entwicklungen, Trends und Phänomene abzielt.

Das Forschungsfeld kämpft nach wie vor mit rechtlichen, ethischen und technologischen Hürden, die einen Zugang zu Social-Media-Daten erschweren. Andererseits konnten Forscher:innen vielfältige Methoden entwickeln, mit denen plattformübergreifende Untersuchungen des Verhaltens der Nutzer:innen und der Inhalte möglich sind. Dazu zählen beispielsweise Methoden, mit denen die Auswirkungen von algorithmischen Empfehlungssystemen hinsichtlich bestimmter Arten von Inhalten bewertet werden können. Gleichzeitig zeigt der vorliegende Bericht, dass der Zugriff auf Social-Media-Daten und deren Weitergabe neue datenschutzrechtliche Risiken für die Nutzer:innen mit sich bringen können, wenn keine ausreichenden technischen und organisatorischen Sicherheitsvorkehrungen getroffen werden. Die Erwartungen der Nutzer:innen an den Datenschutz und die sich darauf beziehenden Regelungen der DSGVO der EU sind daher im Zusammenhang mit dem Datenzugang für die im öffentlichen Interesse liegende Forschung von zentraler Bedeutung.

Darüber hinaus sollte eine Infrastruktur für den Datenzugang gewährleistet werden, die eine sorgfältige Prüfung von Forscher:innen und deren Anträge auf Datenzugang sicherstellt und dabei nicht nur die Datenschutzverpflichtungen berücksichtigt, sondern auch für mehr Klarheit und Kohärenz in der Social-Media-Forschung sorgen kann. Dadurch ließen sich ebenfalls die Vergleichbarkeit und Überprüfung der Forschungsergebnisse im Rahmen von Peer-Reviews verbessern.

Anstatt Maßnahmen zu duplizieren oder neu zu erfinden, sollten Plattformen, politische Entscheidungsträger:innen, Aufsichtsbehörden und Forscher:innen gemeinsame Prozesse nutzen, die auf bestehenden Initiativen aufbauen. Der von der Arbeitsgruppe der *EDMO* ausgearbeitete Entwurf für Verhaltensregeln und die geplante unabhängige Vermittlungsstelle bieten Ansätze, die auf die internationale Zusammenarbeit zwischen liberal-demokratischen Staaten außerhalb der EU ausgeweitet werden könnten. Politische Entscheidungsträger:innen, Aufsichtsbehörden und Forscher:innen müssen zusammenarbeiten und ihre jeweilige Expertise einbringen, um Vertrauen zwischen den Beteiligten aufzubauen und sicherzustellen, dass die Datenzugangsregelungen auf einem soliden Rechtsrahmen beruhen, der die sozialwissenschaftliche Grundlagenforschung unterstützt. Diese Zusammenarbeit sollte nicht nur eine evidenzbasierte Regulierung ermöglichen, sondern auch die wissenschaftliche Forschung im digitalen Zeitalter allgemein fördern. Um die Machbarkeit der geplanten Datenzugangsregelungen zu gewährleisten und etwaige Hindernisse bei der technischen Umsetzung frühzeitig zu erkennen, sollten auch Mitarbeiter:innen der Plattformen, die in Bereichen wie der Produktentwicklung arbeiten, in den gesamten Prozess eingebunden werden.

Letztlich sollten alle empfohlenen Schritte seitens der Stakeholder auf Akzeptanz stoßen, was neben klaren Aufsichtsmechanismen auch die aktive Bereitschaft aller Beteiligten erfordert. Dabei sollte das Ziel im Vordergrund stehen, eine vertrauensvolle, transparente und kooperative Beziehung zwischen politischen Entscheidungsträger:innen, Aufsichtsbehörden, Forscher:innen und Unternehmen zu fördern. Durch diese vereinten Anstrengungen kann eine *Community of Practice* entstehen, die sich über die gemeinsame Mission definiert, neues Wissen aus Social-Media-Daten zu gewinnen und einen Beitrag zur politischen Entscheidungsfindung in liberal-demokratischen Staaten zu leisten, damit diese den Herausforderungen des digitalen Zeitalters gewachsen sind.

Endnoten

1 Persily, N. (2022). Platform Transparency: Understanding the Impact of Social Media. Testimony Before the United States Senate Committee on the Judiciary – Subcommittee on Privacy, Technology, and the Law. Abrufbar unter: https://www.judiciary.senate.gov/imo/media/doc/Persily%20Testimony.pdf

2 Vgl. z. B. Haugen, F. (2021). Statement. United States Senate Committee on Commerce, Science and Transportation – Sub-Committee on Consumer Protection, Product Safety, and Data Security. Abrufbar unter: https://www.commerce.senate.gov/services/files/FC8A558E-824E-4914-BEDB-3A7B1190BD49

3 Vgl. z. B. § 2 Netzwerkdurchsetzungsgesetz (NetzDG) in Bezug auf die Berichtspflichten. Abrufbar unter: https://www.gesetze-im-internet.de/netzdg/BJNR335210017.html

4 Kupferschmidt, K. (2023). Twitter's plan to cut off free data access evokes 'fair amount of panic' among scientists. *Science*. Abrufbar unter: https://www.science.org/content/article/twitters-plan-cut-free-data-access-evokes-fair-amount-panic-among-scientists

5 Vgl. z. B.: An Open Letter to Mr. Mark Zuckerberg: A Global Call to Act Now on Child and Adolescent Mental Health Science. *Oxford Internet Institute (OII)*. Abrufbar unter: https://www.oii.ox.ac.uk/an-open-letterto-mark-zuckerberg/, oder Pasquetto, I. et al. (2020). Tackling misinformation: What researchers could do with social media data. *Harvard Kennedy School Misinformation Review*. Abrufbar unter: https://misinforeview.hks.harvard.edu/article/tackling-misinformation-what-researchers-coulddo-with-social-media-data/

6 So schreibt Artikel 15 des Gesetzes über digitale Dienste (DSA) vor, dass Angaben in Transparenzberichten nach der Art der rechtswidrigen Inhalte oder des Verstoßes gegen die allgemeinen Geschäftsbedingungen des Diensteanbieters aufgeschlüsselt werden müssen. Siehe dazu: Amtsblatt der Europäischen Union (2022). Verordnung (EU) 2022/2065 des Europäischen Parlaments und des Rates vom 19. Oktober 2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG (Gesetz über digitale Dienste) 65. Jahrgang. 27 Oktober 2022. Abrufbar unter: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065&from=EN

7 Bei Elizabeth Hansen Shapiro et al. wird diese Kategorie als Platform Moderation Data [Moderationsrichtlinien, Daten zu moderierten Inhalten, Daten zu koordiniertem unauthentischen Verhalten *(CIB)*] bezeichnet und von der Kategorie *Platform Distribution Data* (Daten zum Anzeigen-Targeting, Daten zu Suchergebnissen, Algorithmen für die Empfehlung von Inhalten und Daten zur Nutzererfahrung) unterschieden. Siehe dazu: Hansen Shapiro, E., Sugarman, M., Bermejo, F. und Zuckerman, E. (2021). Researcher Access to Platform Data: *NetGain Partnership*. Abrufbar unter: https://drive.google.com/file/d/1bPsMbaBXAROUYVesaN3dCtfaZpXZgl0x/view

8 Coldewey, D. (2022). Musk's 'Twitter Files' offer a glimpse of the raw, complicated and thankless task of moderation. *Techcrunch*. Abrufbar unter: https://techcrunch.com/2022/12/09/musks-twitter-files-offer-a-glimpse-of-the-raw-complicated-and-thankless-task-of-moderation/?guccounter=1

9 DiResta, R., Edelson, L., Nyhan, B. und Zuckerman, E. (2022). It's Time to Open the Black Box of Social Media. *Scientific American*. Abrufbar unter: https://www.scientificamerican.com/article/its-time-to-open-the-black-box-of-social-media/

10 Ebd.

11 Pasquetto, I. et al. (2020). Tackling misinformation: what researchers could do with social media data. *Harvard Kennedy School Misinformation Review*. Verfügbar unter: https://misinforeview.hks.harvard.edu/article/tackling-misinformation-what-researchers-could-do-with-social-media-data/

12 Thorburn, L. (2022). What Will "Amplification" Mean in Court?. *Tech Policy Press*. Abrufbar unter: https://techpolicy.press/what-will-amplification-mean-in-court/

13 Vgl. z.B. Matlach, P., Hammer, D. und Schwieter, C. (2022) Auf Odysee: Die Rolle von Blockchain-Technologie für die Monetarisierung im rechtsextremen Onlinemilieu. *Institute for Strategic Dialogue (ISD)*. Abrufbar unter: https://www.isdglobal.org/isd-publications/auf-odysee-die-rolle-von-blockchain-technologie-fur-die-monetarisierung-in-rechtsextremen-onlinemilieu/

14 Guhl, J., Marsh, O. und Tuck, H. (2022). Erforschung des sich im Wandel begriffenen Online-Ökosystems: Hindernisse, Methoden und zukünftige Herausforderungen. *Institute for Strategic Dialogue (ISD)*. Abrufbar unter: https://www.isdglobal.org/isd-publications/researching-the-evolving-online-ecosystem-barriers-methods-and-future-challenges/

15 Hammer, D., Rübbert, Z. und Schwieter, C. (2022). Im toten Winkel – Wie Rechtsextreme alternative Online-Plattformen zur Radikalisierung nutzen. Konferenzbericht zur Jahreskonferenz 2021 des Projekts »Radikalisierung in rechtsextremen Online-Subkulturen entgegentreten«. *Institute for Strategic Dialogue (ISD)*. Abrufbar unter: https://isdgermany.org/im-toten-winkel-wie-rechtsextreme-alternative-online-plattformen-zur-radikalisierung-nutzen/

16 Ahmed, W. (2019). Using Twitter as a data source: an overview of social media research tools. *LSE*

Impact Blog. Abrufbar unter: https://blogs.lse.ac.uk/impactofsocialsciences/2019/06/18/using-twitter-as-a-data-source-an-overview-of-social-media-research-tools-2019/
17 Guhl, J., Marsh, O. und Tuck, H. (2022). Erforschung des sich im Wandel begriffenen Online-Ökosystems: Hindernisse, Methoden und zukünftige Herausforderungen. *Institute for Strategic Dialogue (ISD)*. Abrufbar unter: https://www.isdglobal.org/isd-publications/researching-the-evolving-online-ecosystem-barriers-methods-and-future-challenges/
18 Camargo, C. Q. und Simon, F. M. (2022). Mis- and disinformation studies are too big to fail: six suggestions for the field's future. *Harvard Kennedy School Misinformation Review*. September 2022, Volume 3, Issue 5. Abrufbar unter: https://misinforeview.hks.harvard.edu/article/mis-and-disinformation-studies-are-too-bigto-fail-six-suggestions-for-the-fields-future/
19 Kinder-Kurlanda, K. E. und Weller, K. (2020). Perspective: Acknowledging Data Work in the Social Media Research Lifecycle. *Frontiers in Big Data*. Volume 3 – 2020. Abrufbar unter: https://doi.org/10.3389/fdata.2020.509954
20 Verhulst, S. G. et al. (2019). Leveraging private data for public good. A Descriptive Analysis and Typology of Existing Practices. *GovLab*. Abrufbar unter: https://thegovlab.org/static/files/publications/data-collab-report_Oct2019.pdf
21 Hammer, H., Gerster, L. und Schwieter, C. (2023). Im digitalen Labyrinth: Rechtsextreme Strategien der Dezentralisierung im Netz und mögliche Gegenmaßnahmen. *Institute for Strategic Dialogue (ISD)*. Abrufbar unter: https://www.isdglobal.org/isd-publications/inside-the-digital-labyrinth/
22 Kinder-Kurlanda, K. E. und Weller, K. (2020). Perspective: Acknowledging Data Work in the Social Media Research Lifecycle. *Frontiers in Big Data*. Volume 3 – 2020. Abrufbar unter: https://doi.org/10.3389/fdata.2020.509954
23 Hammer, D., Rübbert, Z. und Schwieter, C. (2022). Im toten Winkel – Wie Rechtsextreme alternative Online-Plattformen zur Radikalisierung nutzen. Konferenzbericht zur Jahreskonferenz 2021 des Projekts »Radikalisierung in rechtsextremen Online-Subkulturen entgegentreten«. *Institute for Strategic Dialogue (ISD)*. Abrufbar unter: https://isdgermany.org/im-toten-winkel-wie-rechtsextreme-alternative-online-plattformen-zur-radikalisierung-nutzen/
24 Europäische Kommission (2022). 2022 Strengthened Code of Practice on Disinformation. *Europäische Kommission*. Abrufbar unter: https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation
25 Transparency Centre (2023). Reports Archive. Abrufbar unter: https://disinfocode.eu/reports-archive/?years=2023
26 Google (2010). Greater transparency around government requests. *Official Blog*. Abrufbar unter: https://googleblog.blogspot.com/2010/04/greater-transparency-around-government.html
27 The Santa Clara Principles On Transparency and Accountability in Content Moderation. Abrufbar unter: https://santaclaraprinciples.org/
28 Singh, S. und Leila Doty, L. (2021). The Transparency Report Tracking Tool: How Internet Platforms Are Reporting on the Enforcement of Their Content Rules. *Open Technology Institute*. Abrufbar unter: https://www.newamerica.org/oti/reports/transparency-report-tracking-tool/
29 Gleicher, N., Nimmo, B., Agranovich, D. und Dvilyanski, M. (2021). Adversarial Threat Report. Meta/ Facebook. Abrufbar unter: https://about.fb.com/wp-content/uploads/2021/12/Metas-Adversarial-Threat-Report.pdf
30 European Commission (2023). Digital Services Act: Commission designates first set of Very Large Online Platforms and Search Engines. Abrufbar unter: https://ec.europa.eu/commission/presscorner/detail/en/ip_23_2413
31 Das New America's Open Technology Institute hat beispielsweise ein Toolkit für die Transparenzberichterstattung vorgeschlagen, das sich auf staatliche Aufforderungen zur Herausgabe von Nutzer:innen-Daten und auf die Berichterstattung über gelöschte Inhalte konzentriert. Ähnliche Maßnahmen wurden von anderen relevanten Stakeholdern initiiert. Beispiele sind die Richtlinien zur Transparenzberichtserstattung von Tech against Terrorism für staatliche Instanzen oder das Voluntary Transparency Reporting Framework, das von der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) entwickelt wurde.
32 Hansen Shapiro, E., Sugarman, M., Bermejo, F. und Zuckerman, E. (2021). Researcher Access to Platform Data: *NetGain Partnership*. Abrufbar unter: https://drive.google.com/file/d/1bPsMbaBXAROUYVesaN3dCtfaZpXZgl0x/view
33 Social Science One (2018). Public Launch. *Harvard's Institute for Quantitative Social Science*. Abrufbar unter: https://socialscience.one/blog/social-science-one-public-launch

34 Schrage, E. und Ginsberg, D. (2018). Facebook Launches New Initiative to Help Scholars Assess Social Media's Impact on Elections. Facebook Newsroom. *Meta.* Abrufbar unter: https://about.fb.com/news/2018/04/new-elections-initiative/

35 Social Science One (2018). Public Launch. *Harvard's Institute for Quantitative Social Science.* Abrufbar unter: https://socialscience.one/blog/social-science-one-public-launch

36 King, G. und Persily, N. (2020). A New Model for Industry–Academic Partnerships. *PS: Political Science & Politics,* 53(4), 703-709. doi:10.1017/S1049096519001021. Abrufbar unter: https://www.cambridge.org/core/journals/ps-political-science-and-politics/article/new-model-for-industryacademic-partnerships/AD7D0B8EA582DC017D9A24754D833CAA

37 King, G. und Persily, N. (2020). Unprecedented Facebook URLs Dataset now Available for Academic Research through Social Science One. *Harvard's Institute for Quantitative Social Science.* Abrufbar unter: https://socialscience.one/blog/unprecedented-facebook-urls-dataset-now-available-research-through-social-science-one

38 Ebd.

39 Evans, G. und King, G. (2022). Statistically Valid Inferences from Differentially Private Data Releases, with Application to the Facebook URLs Dataset. Political Analysis, S. 1-21. Abrufbar unter: https://tinyurl.com/yc5mx3sw; Evans, G. King, G., Schwenzfeier, M. und Thakurta, A. (2020). Statistically Valid Inferences from Privacy Protected Data. *American Political Science Review.* Abrufbar unter: https://tinyurl.com/yd4xbnb8

40 King, G. und Persily, N. (2020). Unprecedented Facebook URLs Dataset now Available for Academic Research through Social Science One. *Harvard's Institute for Quantitative Social Science.* Abrufbar unter: https://socialscience.one/blog/unprecedented-facebook-urls-dataset-now-available-research-through-social-science-one

41 Persily, N. (2022). Platform Transparency: Understanding the Impact of Social Media. Testimony Before the United States Senate Committee on the Judiciary – Subcommittee on Privacy, Technology, and the Law. Abrufbar unter: https://www.judiciary.senate.gov/imo/media/doc/Persily%20Testimony.pdf

42 Ebd.

43 Vogus, C. (2023). Defending Data: Privacy Protection, Independent Researchers, and Access to Social Media Data in the US and EU. *Center for Democracy & Technology (CDT).* Abrufbar unter: https://cdt.org/wp-content/uploads/2023/01/2023-01-23-CDT-Defending-Data-Independent-Researcher-Access-to-Data-report-final.pdf

44 Erwägungsgrund 47 der DSGVO spricht von den »vernünftigen Erwartungen« der betroffenen Personen (*data subjects*), die auf ihrer Beziehung zu dem Verantwortlichen (*controller*) beruhen. Vgl. Proton AG (2023). What is GDPR, the EU's new data protection law?. GDRP.EU. Abrufbar unter: https://gdpr.eu/what-is-gdpr/

45 Artikel 40, Amtsblatt der Europäischen Union (2022). Verordnung (EU) 2022/2065 des Europäischen Parlaments und des Rates vom 19. Oktober 2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG (Gesetz über digitale Dienste) 65. Jahrgang. 27 Oktober 2022. Abrufbar unter: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065&from=EN

46 Vermeulen, M. (2022). Researcher Access to Platform Data: European Developments. *Journal of Online Trust and Safety. Vol. 1 No. 4 (2022).* Abrufbar unter: https://tsjournal.org/index.php/jots/article/view/84/31

47 Europäische Kommission (2022). 2022 Strengthened Code of Practice on Disinformation. *Europäische Kommission.* Abrufbar unter: https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation

48 NYU Cybersecurity for Democracy (2022). Transparency For "Reasonably Public" Platform Content. Why we need transparency of certain types of public, high reach content. Policy Overview. *NYU Cybersecurity for Democracy.* Abrufbar unter: https://cybersecurityfordemocracy.cdn.prismic.io/cybersecurityfordemocracy/532dcdca-27dc-478b-b579-411d82b7e903_20220505_C4D_HighEngagement_sum_v5.pdf.

49 Vermeulen, M. (2022). Researcher Access to Platform Data: European Developments. *Journal of Online Trust and Safety.* Vol. 1 No. 4 (2022). Abrufbar unter: https://tsjournal.org/index.php/jots/article/view/84/31

50 Europäische Kommission (2022). 2022 Strengthened Code of Practice on Disinformation. Europäische Kommission. Abrufbar unter: https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation

51 CrowdTangle (2023). What data is CrowdTangle tracking? Abrufbar unter: https://help.crowdtangle.com/en/articles/1140930-what-data-is-crowdtangle-tracking

52 Alba, D. (2022). Meta Pulls Support for Tool Used to Keep Misinformation in Check. *Bloomberg.* Abrufbar unter: https://www.bloomberg.com/news/articles/2022-06-23/meta-pulls-support-for-tool-used-to-keep-misinformation-in-check?leadSource=uverify%20wall

53 Roose, K. (2021). Inside Facebook's Data Wars. *New York Times*. Abrufbar unter: https://www.nytimes.com/2021/07/14/technology/facebook-data.html
54 Albert, J. (2022). Facebook's gutting of CrowdTangle: a step backward for platform transparency. *AlgorithmWatch*. Abrufbar unter: https://algorithmwatch.org/en/crowdtangle-platform-transparency/
55 Meta (2022). Widely Viewed Content Report: What People See on Facebook. Q4 2022 report. *Transparency Center*. Abrufbar unter: https://transparency.fb.com/data/widely-viewed-content-report/
56 Vogus, C. (2022). Improving Researcher Access to Digital Data. A Workshop Report. *Center for Democracy & Technology (CDT)*. Abrufbar unter: https://cdt.org/wp-content/uploads/2022/08/2022-08-15-FX-RAtD-workshop-report-final-int.pdf
57 Vogus, C. (2023). Defending Data: Privacy Protection, Independent Researchers, and Access to Social Media Data in the US and EU. *Center for Democracy & Technology (CDT)*. Abrufbar unter: https://cdt.org/wp-content/uploads/2023/01/2023-01-23-CDT-Defending-Data-Independent-Researcher-Access-to-Data-report-final.pdf
58 Mozilla (2021). YouTube Regrets. A crowdsourced investigation into YouTube's recommendation algorithm. *foundation.mozilla.org*. Abrufbar unter: https://assets.mofoprod.net/network/documents/Mozilla_YouTube_Regrets_Report.pdf
59 Ricks, B. und McCrosky, J. (2022). Does This Button Work? Investigating YouTube's ineffective user controls. *foundation.mozilla.org*. Abrufbar unter: https://assets.mofoprod.net/network/documents/Mozilla-Report-YouTube-User-Controls.pdf
60 Edelson, L. et al. (2021). Researchers, NYU, Knight Institute Condemn Facebook's Effort to Squelch Independent Research about Misinformation. Presseerklärung. *Knight First Amendment Institute*. Abrufbar unter: https://knightcolumbia.org/content/researchers-nyu-knight-institute-condemn-facebooks-effort-to-squelch-independent-research-about-misinformation
61 Erwin, M. (2021). Why Facebook's claims about the Ad Observer are wrong. *The Mozilla Blog*. Abrufbar unter: https://blog.mozilla.org/en/mozilla/news/why-facebooks-claims-about-the-ad-observer-are-wrong/
62 Coons, C. (2022). Senator Coons, colleagues introduce legislation to provide public with transparency of social media platforms. *Presseerklärung*. Abrufbar unter: https://www.coons.senate.gov/news/press-releases/senator-coons-colleagues-introduce-legislation-to-provide-public-with-transparency-of-social-media-platformshttps://www.coons.senate.gov/news/press-releases/senator-coons-colleagues-introduce-legislation-to-provide-public-with-transparency-of-social-media-platforms
63 Vogus, C. (2022). Improving Researcher Access to Digital Data. A Workshop Report. *Center for Democracy & Technology (CDT)*. Abrufbar unter: https://cdt.org/wp-content/uploads/2022/08/2022-08-15-FX-RAtD-workshop-report-final-int.pdf
64 Mozilla. Abrufbar unter: https://blog.mozilla.org/security/2018/08/01/safe-harbor-for-security-bug-bounty-participants/
65 In dem gestärkten Verhaltenskodex schließt »Desinformation« die Begriffe »Fehlinformation«, »Desinformation«, »Einflussnahme auf Informationen« sowie »Einmischungen aus dem Ausland in den Informationsraum« ein, die im Europäischen Aktionsplan für Demokratie der Europäischen Kommission definiert werden (S. 18). Abrufbar unter: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0790&from=EN
66 Transparency Centre (2023). Abrufbar unter: https://disinfocode.eu/
67 Proton AG (2023). What is GDPR, the EU's new data protection law?. *GDRP.EU*. Abrufbar unter: https://gdpr.eu/what-is-gdpr/
68 EDMO (2022). Report of the European Digital Media Observatory's Working Group on Platform-to-Researcher Data Access. *European Digital Media Observatory (EDMO)*. Abrufbar unter: https://edmoprod.wpengine.com/wp-content/uploads/2022/02/Report-of-the-European-Digital-Media-Observatorys-Working-Group-on-Platform-to-Researcher-Data-Access-2022.pdf
69 Als Reaktion auf einen Aufruf zur Stakeholder-Beteiligung im November 2020 haben Tech-Unternehmen Kommentare zur Absicht der EDMO abgegeben, eine Arbeitsgruppe zum Thema »Zugang zu Plattformdaten für sozialwissenschaftliche Zwecke« einzusetzen. Die Kommentare von Meta können beispielsweise unter dem folgenden Link eingesehen werden. Abrufbar unter: https://about.fb.com/wp-content/uploads/2020/12/Facebook-Response-to-EDMO-Request-for-Submissions.pdf
70 Abrufbar unter: EDMO (2022). Report of the European Digital Media Observatory's Working Group on Platform-to-Researcher Data Access. *European Digital Media Observatory (EDMO)*. Abrufbar unter: https://edmoprod.wpengine.com/wp-content/uploads/2022/02/Report-of-the-European-Digital-Media-Observatorys-Working-Group-on-Platform-to-Researcher-Data-Access-2022.pdf
71 Ebd.

72 EDPS (2020). A Preliminary Opinion on data protection and scientific research. *European Data Protection Supervisor (EDPS)*. Abrufbar unter: https://edps.europa.eu/sites/default/files/publication/20-01-06_opinion_research_en.pdf
73 EDMO (2022). Report of the European Digital Media Observatory's Working Group on Platform-to-Researcher Data Access. *European Digital Media Observatory (EDMO)*. Abrufbar unter: https://edmoprod.wpengine.com/wp-content/uploads/2022/02/Report-of-the-European-Digital-Media-Observatorys-Working-Group-on-Platform-to-Researcher-Data-Access-2022.pdf
74 Amtsblatt der Europäischen Union (2022). Verordnung (EU) 2022/2065 des Europäischen Parlaments und des Rates vom 19. Oktober 2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG (Gesetz über digitale Dienste, *Digital Services Act, DSA*) 65. Jahrgang. 27 Oktober 2022. Abrufbar unter: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065&from=EN
75 Vermeulen, M. (2022). Researcher Access to Platform Data: European Developments. *Journal of Online Trust and Safety*. Vol. 1 No. 4 (2022). Abrufbar unter: https://tsjournal.org/index.php/jots/article/view/84/31
76 Schwieter, C. (2022). Online-Krisenprotokolle – Erweiterung des Politikinstrumentariums zum Schutz der Demokratie in Krisensituationen. *Institute for Strategic Dialogue (ISD)*. Abrufbar unter: https://isdgermany.org/wp-content/uploads/2022/12/ISD_policy-brief2-de_221213_vfinal.pdf
77 EDMO (2022). Report of the European Digital Media Observatory's Working Group on Platform-to-Researcher Data Access. E*uropean Digital Media Observatory (EDMO)*. Abrufbar unter: https://edmoprod.wpengine.com/wp-content/uploads/2022/02/Report-of-the-European-Digital-Media-Observatorys-Working-Group-on-Platform-to-Researcher-Data-Access-2022.pdf
78 Vermeulen, M. (2022). Researcher Access to Platform Data: European Developments. *Journal of Online Trust and Safety*. Vol. 1 No. 4 (2022). Abrufbar unter: https://tsjournal.org/index.php/jots/article/view/84/31
79 Jaursch, J. (2022). Barriers to Strong DSA Enforcement – and How to Overcome Them. *Tech Policy Press*. Abrufbar unter: https://techpolicy.press/barriers-to-strong-dsa-enforcement-and-how-to-overcome-them/
80 Jaursch, J. (2022). Platform oversight. Here is what a strong Digital Services Coordinator should look like. *Verfassungsblog*. Abrufbar unter: https://verfassungsblog.de/dsa-dsc/

ISD | Institute for Strategic Dialogue

Amman | Berlin | London | Paris | Washington DC

www.isdgermany.org

gefördert durch:
Auswärtiges Amt