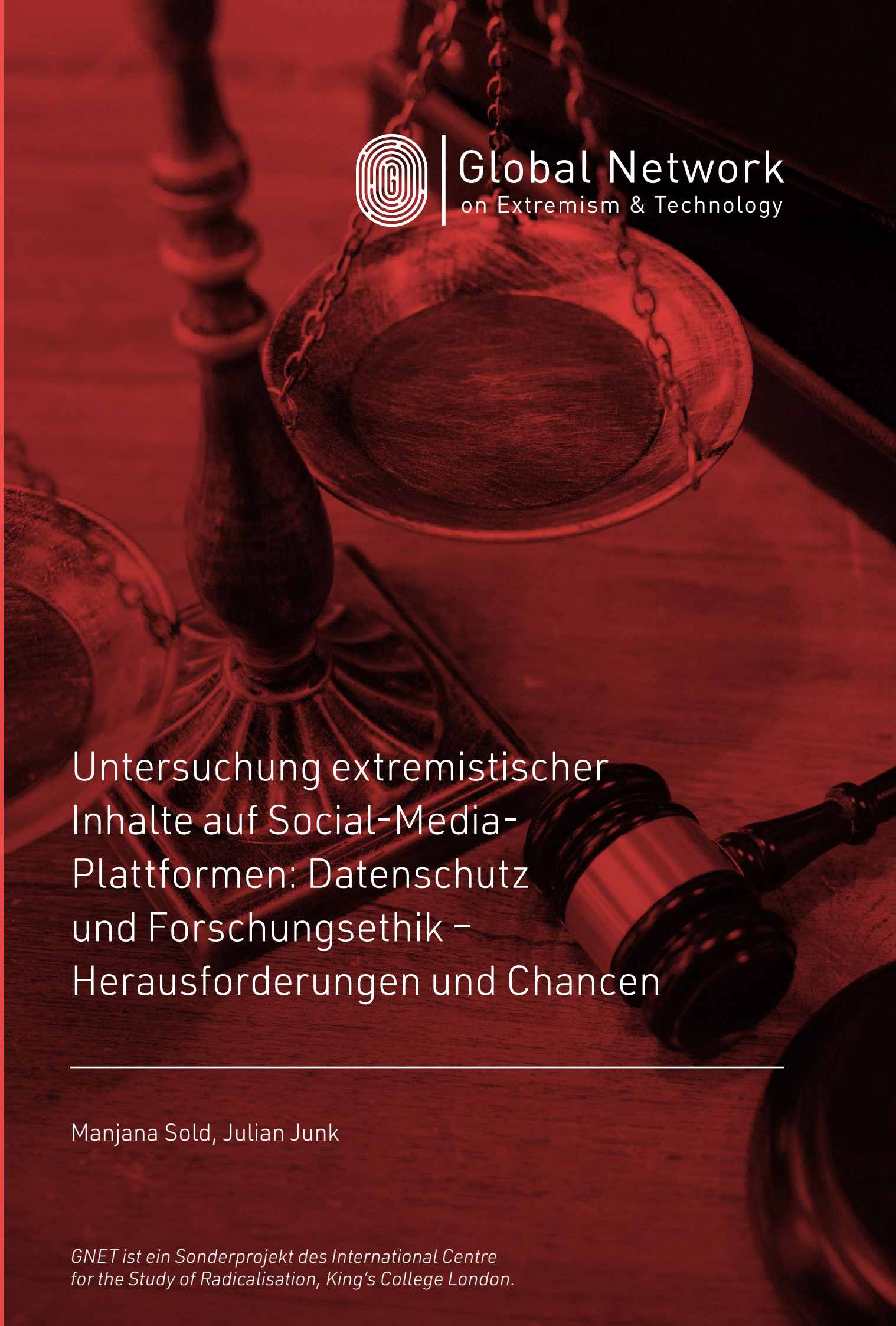

Global Network
on Extremism & Technology

Untersuchung extremistischer Inhalte auf Social-Media-Plattformen: Datenschutz und Forschungsethik – Herausforderungen und Chancen

Manjana Sold, Julian Junk

GNET ist ein Sonderprojekt des International Centre for the Study of Radicalisation, King's College London.

Die Autoren dieses Berichts sind
Manjana Sold und Julian Junk

Das Global Network on Extremism and Technology (GNET) ist eine akademische Forschungsinitiative mit Unterstützung des Global Internet Forum to Counter Terrorism (GIFCT), einer unabhängigen, aber von der Wirtschaft finanzierten Initiative mit dem Ziel, die Nutzung von Technologie für terroristische Zwecke besser zu verstehen und einzudämmen. GNET wird einberufen und geleitet vom International Centre for the Study of Radicalisation (ICSR), einem akademischen Forschungszentrum innerhalb des Department of War Studies am King's College London. Die in diesem Dokument enthaltenen Ansichten und Schlussfolgerungen sind den Autoren zuzuschreiben und sollten nicht als die ausdrücklichen oder stillschweigenden Ansichten und Schlussfolgerungen von GIFCT, GNET oder ICSR verstanden werden.

KONTAKTANGABEN

Im Falle von Fragen oder zur Anforderung weiterer Exemplare wenden Sie sich bitte an:

ICSR
King's College London
Strand
London WC2R 2LS
Vereinigtes Königreich

T. **+44 20 7848 2098**
E. **mail@gnet-research.org**

Twitter: **@GNET_research**

Wie alle anderen GNET-Publikationen kann auch dieser Bericht kostenlos von der GNET-Website unter www.gnet-research.org heruntergeladen werden.

Kurzfassung

Der Nexus zwischen Terrorismus und Technologie ist gesellschaftlich und politisch relevanter denn je. So gut wie jeder Mobilisierungs- und Radikalisierungsprozess und praktisch alle gewalttätigen Angriffe – ob durchgeführt oder verhindert – haben eine Online-Komponente. Die Forschenden, nicht zuletzt die am GNET beteiligten, arbeiten intensiv daran, diese Prozesse in den empirisch anspruchsvollen Online-Umgebungen zu analysieren. Trotz der sich ständig ändernden Plattformen und Richtlinien sowie der Verlagerung in immer stärker geschlossene und verschlüsselte Räume gibt es reichlich empirische Daten. Die Datenfülle bringt eigene Herausforderungen und Chancen mit sich.[1] Dabei gibt es jedoch klare Grenzen sowie Grauzonen im Hinblick darauf, was Forschende, die sich mit extremistischen Online-Inhalten beschäftigen, tun können und dürfen, denn hier kommen ethische und datenschutzrechtliche Aspekte ins Spiel. Die Diskussionen zu diesen Themen haben in den vergangenen Jahren stark an Relevanz gewonnen und werden besonders in internationalen Forschungskonsortien lebhaft geführt.

Der vorliegende GNET-Bericht fasst den Stand der Diskussion um Ethik und Datenschutz zusammen, zeigt die Grenzen und Möglichkeiten der Forschung auf und formuliert entsprechende Empfehlungen für Forschende und Technologieunternehmen. Er geht dabei in drei Schritten vor: Er umreißt zunächst einige der wichtigsten ethischen Überlegungen, die Forschende in diesem akademischen Bereich anstellen müssen. Des Weiteren liefert er einen Überblick über die wichtigsten einzuhaltenden Datenschutzprinzipien und zeigt die Möglichkeiten und Konflikte auf, denen Forschende in diesem Zusammenhang ausgesetzt sind; Zuletzt erörtert er das Zusammenspiel von Forschenden, Datenquellen und Plattformrichtlinien und fasst die Erkenntnisse in diesem Zusammenhang zu einigen wichtigen Empfehlungen für Forschung, Technologieunternehmen und Regulierungsbehörden zusammen. Die wichtigsten Punkte: Erstens würden mehr plattformübergreifende Zugangspunkte und Datenbanken Anreize für ein breiteres und dynamischeres Forschungsfeld bieten. Zweitens würde die dringend notwendige internationale Forschungszusammenarbeit zur Analyse extremistischer Online-Inhalte von einer stärkeren internationalen Harmonisierung und einer Konvergenz der Datenschutzbestimmungen profitieren. Drittens dürfen die Datenschutzregelungen nicht als Unannehmlichkeit betrachtet werden, sondern als Voraussetzung für die Forschung, indem sie klarer abgrenzen, was möglich ist und was nicht. Und nicht zuletzt erfordert das dynamische empirische Feld Mechanismen des regelmäßigen Austauschs zwischen Technologieunternehmen, Forschung und Regulierungsbehörden, um Grundsätze, Gepflogenheiten und rechtliche Rahmenbedingungen in einer Weise anzupassen, die der sozialen und politischen Relevanz des Nexus zwischen Extremismus und Technologie gerecht wird.

1 Abdullah Alrhmoun, Shiraz Maher und Charlie Winter, *Hass decodieren: Klassifizierung terroristischer Inhalte mittels experimenteller Textanalyse*, ICSR King's College London (2020).

Inhalt

1 Einleitung

Der digitale Raum hat in den Radikalisierungsprozessen vieler Täter vergangener Anschläge eine zentrale Rolle gespielt:[1] Extremisten wie Anis Amri (Berlin, Deutschland), Brenton Tarrant (Christchurch, Neuseeland) und Stephan Balliet (Halle, Deutschland) haben Social-Media-Plattformen nicht nur genutzt, um Informationen zu sammeln und zu verbreiten, sich zu vernetzen und zu inszenieren, sondern auch, um sich mit Gleichgesinnten auszutauschen und teilweise sogar, um einen Livestream des Anschlags mit Tausenden von Zuschauern zu teilen. Durch diese Kommunikation radikaler oder extremistischer Akteure können wir viel über die Radikalisierungsprozesse lernen, die in der virtuellen Welt stattfinden. Der Content und seine Darstellung sowie die Art und Weise, wie diese Akteure kommunizieren, sind dabei von zentraler Bedeutung und können als Ausgangspunkt für die Entwicklung der effektivsten präventiven und demobilisierenden Maßnahmen dienen.

Im Rahmen dieses Forschungsfeldes haben Daten, die aus sozialen Medien gewonnen werden, natürlich an Bedeutung gewonnen.[2] Das zeigen zahlreiche wissenschaftliche Publikationen, die auf Daten aus sozialen Medien basieren, beispielsweise Facebook,[3] Twitter,[4] YouTube[5] und Instagram.[6] Es kann nun auf einen extrem großen Datenbestand zugegriffen werden, der zur Entwicklung und Prüfung von Hypothesen genutzt werden kann.[7] Allerdings gehen mit diesen Möglichkeiten auch Einschränkungen und Fallstricke einher. Hierbei geht es um mögliche ethische und datenschutzrechtliche Anforderungen, die sicherlich eine Herausforderung für die Forschung darstellen, aber auch viele Chancen bieten. Neben der unerlässlichen Transparenz und der Leitlinie „Maximierung des Nutzens bei

1 Wir sind Sebastian Golla für seine Kommentare zu früheren Versionen dieses Berichts und seine kompetente juristische Begleitung so vieler unserer Forschungsbemühungen in den vergangenen Jahren zu großem Dank verpflichtet. Wir danken außerdem Clara-Auguste Süß für ihre Kommentare sowie Leo Bauer und Klara Sinha für ihre Unterstützung bei der Fertigstellung dieses Berichts.

2 Sebastian J. Golla, Henning Hofmann und Matthias Bäcker, „Connecting the Dots: Sozialwissenschaftliche Forschung in Sozialen Online-Medien im Lichte von DS-GVO und BDSG-neu“, *Datenschutz und Datensicherheit – DuD* 42, Nr. 2 (2018): 89, http://link.springer.com/10.1007/s11623-018-0900-x; Manjana Sold, Hande Abay Gaspar und Julian Junk, Designing Research on Radicalisation using Social Media Content: Data Protection Regulations as Challenges and Opportunities, 2020.

3 Agata Błachnio, Aneta Przepiórka und Patrycja Rudnicka, „Psychological Determinants of Using Facebook: A Research Review“, *International Journal of Human-Computer Interaction* 29 (2013), https://doi.org/10.1080/10447318.2013.780868; Ralf Caers et al., „Facebook: A Literature Review“, *New Media & Society* 15 (2013), https://doi.org/10.1177/1461444813488061; Stefania Manca und Maria Ranieri, „Is It a Tool Suitable for Learning? A Critical Review of the Literature on Facebook as a Technology Enhanced Learning Environment“, *Journal of Computer Assisted Learning* 29 (2013), https://doi.org/10.1111/jcal.12007; Ashwini Nadkarni und Stefan G. Hofmann, „Why do People Use Facebook?“, *Personality and Individual Differences* 52, Nr. 3 (2012), https://doi.org/10.1016/j.paid.2011.11.007; Robert E. Wilson, Samuel D. Gosling und Lindsay T. Graham, „A Review of Facebook Research in the Social Sciences“, *Perspectives on Psychological Science* 7 (2012), https://doi.org/10.1177/1745691612442904.

4 Jytte Klausen, „Tweeting the Jihad: Social Media Networks of Western Foreign Fighters in Syria and Iraq“, *Studies in Conflict & Terrorism* 38, Nr. 1 (2015); Amandeep Dhir, Khalid Buragga und Abeer A. Boreqqah, „Tweeters on Campus: Twitter a Learning Tool in Classroom?“, *Journal of Universal Computer Science* 19 (2013); Shirley Ann Williams, Melissa Terras und Claire Warwick, „What Do People Study When They Study Twitter? Classifying Twitter Related Academic Papers“, *Journal of Documentation* 69 (2013).

5 Chareen Snelson, „YouTube Across the Disciplines: A Review of the Literature“, *MERLOT Journal of Online Learning and Teaching Journal of Qualitative Methods* 7, Nr. 14 (2011), http://jolt.merlot.org/vol7no1/snelson_0311.htm; Raphael Ottoni et al., „Analyzing Right-wing YouTube Channels: Hate, Violence and Discrimination“, (2018); Kostantinos Papadamou et al., „Understanding the Incel Community on YouTube“, (2020).

6 Tim Highfield und Tama Leaver, „A Methodology for Mapping Instagram Hashtags“, *First Monday* 20, Nr. 1 (2015); Asuncion Bernardez-Rodal, Paula Requeijo Rey und Yanna G. Franco, „Radical right parties and anti-feminist speech on Instagram: Vox and the 2019 Spanish general election“, *Party Politics* (2020); Lena Frischlich, „#Dark inspiration: Eudaimonic entertainment in extremist Instagram posts“, *new media & society* (2020).

7 Golla, Hofmann und Bäcker, „Connecting the Dots: Sozialwissenschaftliche Forschung in Sozialen Online-Medien im Lichte von DS-GVO und BDSG-neu“, 89.

Minimierung des Schadens“ gibt es weitere Grundsätze und Richtlinien, die berücksichtigt werden müssen. In den ersten beiden Abschnitten geben wir einen Überblick über einige wichtige ethische Überlegungen, die bei Forschungsprozessen in diesem akademischen Bereich anzustellen sind, und wir beschreiben die wichtigsten Datenschutzprinzipien, die es einzuhalten gilt.[8] Anschließend zeigen wir die Möglichkeiten und die Konflikte auf, mit denen Forschende in diesem Zusammenhang konfrontiert sind. Im dritten Abschnitt diskutieren wir die Interaktion zwischen Forschenden, Datenquellen und Plattformrichtlinien und kommen zu einigen wichtigen Empfehlungen.

8 In Sold, Abay Gaspar und Junk, „Designing Research on Radicalisation using Social Media Content: Data Protection Regulations as Challenges and Opportunities“ gehen wir auf einige dieser Elemente ausführlicher ein, ebenso wie die Kapitel in de Koning et al. „On Speaking, Remaining Silent and Being Heard: Framing Research, Positionality and Publics in the Jihadi Field“, in *Jihadi Audiovisuality and its Entanglements. Meanings, Aesthetics, Appropriations*, Hrsg. Christoph Günther und Simone Pfeifer (Edinburgh: Edinburgh University Press, 2020) und „Ethics in Gender Online Research: A Facebook Case Study“, in *Jihadi Audiovisuality and its Entanglements. Meanings, Aesthetics, Appropriations*, Hrsg. Christoph Günther und Simone Pfeifer (Edinburgh: Edinburgh University Press, 2020) in demselben Band von Günther und Pfeifer *Jihadi Audiovisuality and its Entanglements. Meanings, Aesthetics, Appropriations* (Edinburgh: Edinburgh University Press, 2020).

2 Zentrale ethische Fragen

Ethische Fragen spielen bei fast jedem Forschungsprojekt eine Rolle. Dabei will die Forschungsethik „die beteiligten Menschen schützen und nicht nur die Einhaltung der gesetzlichen Vorschriften sicherstellen“.[9] Bei der Analyse von Inhalten auf Social-Media-Plattformen sind personenbezogene Daten allgegenwärtig.[10] Dieser Umstand wirft zwar weder völlig neue ethische Fragen auf noch setzt er „anerkannte Normen und Werte der Forschungsethik“ außer Kraft.[11] Dennoch machen der oft recht einfache Zugang zu und die schiere Menge dieser Art von Daten sowie die Geschwindigkeit, mit der sich Plattformen, Kontexte und Ereignisse ändern, es nicht nur zu einer Notwendigkeit, sondern auch zu einer recht großen Herausforderung, genügend Raum für ethische Erwägungen zu schaffen und diese Erwägungen an sich verändernde Plattformen, Visualitäten und Richtlinien anzupassen. Wie bei allen Forschungsprojekten müssen also die gesellschaftlichen und wissenschaftlichen Interessen gegen das Recht des Einzelnen auf Privatsphäre abgewogen werden. Daten aus sozialen Medien bringen jedoch einige besondere Herausforderungen mit sich und sind „ein potenzielles Minenfeld“.[12]

Auch wenn es keine allgemeingültige Richtlinie gibt, wonach ethische Grundsätze zwingend zu beachten sind, werden bestimmte ethische Prinzipien in der Literatur immer wieder als besonders relevant hervorgehoben. Diese Grundsätze lassen sich in drei Kategorien einteilen: An erster Stelle stehen diejenigen, die die Beziehung zwischen dem/der Forschenden und den einzelnen Forschungssubjekten betreffen. In die zweite Kategorie fallen Grundsätze hinsichtlich der gesellschaftlichen Dimension. Die dritte und letzte Kategorie umfasst Grundsätze, die selbstreflexiv sind und die Forschenden selbst betreffen. Wir fassen diese Ergebnisse im Folgenden zusammen, um sie für zukünftige Forschungen zu Extremismus und Technologie leicht zugänglich zu machen.

Ethische Grundsätze, die das einzelne Forschungssubjekt betreffen

Zu den Grundsätzen, die das einzelne Forschungssubjekt betreffen, gehören *Vertraulichkeit* bzw. *Achtung der Person* und *lautere Absicht*. Die Gewährleistung der Vertraulichkeit bedeutet, dass Forschende, die die Identität eines Forschungssubjekts kennen, Maßnahmen dafür ergreifen müssen, dass diese Identität nicht an oder durch andere Personen preisgegeben wird. Wann immer möglich, sollte das Einverständnis eingeholt werden, wenn die Daten einer Person für

9 NESH*A Guide to Internet Research Ethics* (2019), 3, https://www.forskningsetikk.no/en/guidelines/social-sciences-humanities-law-and-theology/a-guide-to-internet-research-ethics/.

10 Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (eine „betroffene Person“) beziehen, siehe Artikel 4 (1) der DSGVO.

11 National Committee for Research Ethics in the Social Sciences and the Humanities NESH, *A Guide to Internet Research Ethics*, 2.

12 Sold, Abay Gaspar und Junk, Designing Research on Radicalisation using Social Media Content: Data Protection Regulations as Challenges and Opportunities, 52; siehe auch: Farina Madita Dobrick et al., *Research Ethics in the Digital Age: Ethics for the Social Sciences and Humanities in Times of Mediatization and Digitization*, Hrsg. Farina Madita Dobrick, Jana Fischer und Lutz M. Hagen (Wiesbaden: Springer VS, 2018), 1.

Forschungszwecke verwendet werden.[13] Die informierte Einwilligung gewährleistet die Wahrung der Persönlichkeitsrechte und des Rechts auf informationelle Selbstbestimmung einer Person. Forschende sind folglich zur Transparenz verpflichtet und müssen dafür sorgen, dass die Probanden wissen, dass sie Gegenstand der Forschung sind, dass sie in verständlicher Form über das bevorstehende Forschungsprojekt informiert werden und dass ihnen die Möglichkeit gegeben wird, einer freiwilligen Teilnahme zuzustimmen oder diese abzulehnen. Wenn es um extremistische Inhalte geht, ist die Einholung einer informierten Einwilligung jedoch alles andere als einfach, da der Versuch, die Zustimmung der Forschungssubjekte einzuholen, die Forschung selbst gefährden kann: Das Wissen, dass ihre Daten beobachtet oder gar analysiert werden, führt oft dazu, dass Menschen ihr Verhalten ändern. Wenn zum Beispiel bestimmte Personen wüssten, dass sie (bzw. ihre Online-Threads, -Posts und -Kommentare) beobachtet werden, würden sie sich möglicherweise anders verhalten, über andere Kanäle kommunizieren, ihre Meinung nicht mehr virtuell äußern oder sie anpassen.

Noch schwieriger wird es, wenn die Daten vieler verschiedener Personen für Forschungszwecke verwendet werden sollen.[14] So ist beispielsweise kaum zu gewährleisten, dass 100.000 Twitter-Nutzer rechtzeitig ihr Einverständnis geben, dass Forschende ihre Daten nutzen dürfen. In solchen Fällen können Forschende einen Opt-out-Ansatz anbieten, durch den Einzelpersonen ihre Einwilligung jederzeit während des Forschungsprojekts zurückziehen können. Der Vorteil ist, dass Forschende nicht im Voraus die Zustimmung aller betroffenen Personen einholen müssen. Diese Möglichkeit bietet sich auch an, wenn die Menge der personenbezogenen Daten relativ gering ist oder wenn die Daten anonymisiert werden. Forschende müssen die gesammelten Daten während der Studie und nach deren Abschluss stets vertraulich behandeln. Ob die Einzelpersonen ihr Einverständnis zur Analyse gegeben haben oder nicht, ist dabei unerheblich. In jedem Fall sollten Forschende die Daten pseudonymisieren oder anonymisieren. Allerdings ist die Anonymisierung meistenteils schwierig[15] und Personen können oft auch nach der Anonymisierung noch identifiziert werden.[16] Forschende müssen sich also fragen, wo und wie die Daten gespeichert werden, ob die verwendete Software vertrauenswürdig ist, wie umfassend die Datenschutzrichtlinie des Softwareanbieters ist und ob beispielsweise ein Verschlüsselungsprogramm notwendig ist.

Darüber hinaus gilt das Prinzip der *lauteren Absicht*: Forschende müssen sicherstellen, dass den Teilnehmenden kein Schaden zugefügt wird und dass die Studie maximalen Nutzen erreicht. Zum Beispiel müssen Forschende bei einer Studie über ausländische Aktivisten dafür sorgen, dass alle Daten so anonymisiert werden, dass die betroffene Person nicht identifiziert werden kann, weil dies möglicherweise zu einer strafrechtlichen Verfolgung oder öffentlichen Verurteilung führen kann. Wenn eine solche Anonymisierung nicht zu gewährleisten ist (beispielsweise aufgrund ständiger Überwachung der Forschenden während der Treffen mit den Teilnehmenden oder

13 NESH, *A Guide to Internet Research Ethics*, 2.
14 Elizabeth Buchanan, „Considering the ethics of big data research: A case of Twitter and ISIS/ISIL", *PLoS ONE* 12, Nr. 12 (2017): 2, https://doi.org/10.1371/journal.pone.0187155.
15 Buchanan, „Considering the ethics of big data research: A case of Twitter and ISIS/ISIL", 4.
16 Matthew J. Salganik, *Bit by Bit. Social Research in the Digital Age* (New Jersey: Princeton University Press, 2018), 40. Idealerweise, und gemäß Erwägungsgrund 26 DSGVO, müssen Personen vollständig nicht identifizierbar sein.

weil die Auslassung der personenbezogenen Daten die Überprüfung von Hypothesen unmöglich machen würde), muss die Studie unter Umständen abgebrochen oder neu konzipiert werden.

Was die Maximierung des Nutzens und die Minimierung der Risiken betrifft, so ist vor allem Letzteres immer noch ein komplexes Unterfangen.[17] Bei der Forschung zu digitalen Themen kann der Nutzen der online gesammelten Daten jedoch mit weniger Aufwand maximiert werden. Gründe dafür sind niedrigschwellige Möglichkeiten der Bereitstellung von Daten und Codes zur Reproduzierbarkeit (z. B. Harvard Dataverse oder GitHub) oder hochwertige Open-Access-Zeitschriften, die ein großes Publikum erreichen (wie die neu gegründete *Global Studies Quarterly* der ISA oder die *Texas National Security Review* der UT Austin).

Ethische Grundsätze, die die gesellschaftliche Dimension betreffen

Die Grundsätze, die sich auf die gesellschaftliche Dimension eines Forschungsprojekts beziehen, sind *Gerechtigkeit*, *Achtung vor dem Gesetz und dem öffentlichen Interesse*. Der Grundsatz *Gerechtigkeit* besagt, dass Forschende die Vor- und Nachteile für verschiedene gesellschaftliche Gruppen, die von einem bestimmten Forschungsprojekt betroffen sind, gegeneinander abwägen müssen. Minderheiten und schwache Gruppen dürfen nicht die Nachteile tragen müssen, während gleichzeitig Mehrheiten und wohlhabende Gruppen die Vorteile genießen.[18]

Dem Grundsatz *Achtung vor dem Gesetz und dem öffentlichen Interesse* zufolge sind für die Forschung relevante Gesetze und Seitenrichtlinien (beispielsweise der Social-Media-Unternehmen) grundsätzlich zu beachten.[19] Ein zentrales Problem bei der digitalen Forschung sind die vielfältigen Zuständigkeiten, die es zu beachten gilt, etwa bei der Erhebung von Daten über politische Extremisten in verschiedenen Ländern. In sehr seltenen Fällen ist jedoch auch ein Verstoß gegen Nutzungsbedingungen möglich. So hat sich die New York University bewusst dafür entschieden, gegen die Nutzungsbedingungen von Facebook zu verstoßen, um Daten über Facebooks Strategie für politische Werbung zu erheben, vermutlich weil Facebook sich nach wie vor weigert, Forschenden diese Daten zur Verfügung zu stellen.[20] Da politische Werbung und Desinformation im digitalen Bereich wichtige Faktoren im Zusammenhang mit der Integrität von Wahlen und besserer Demokratie sind und die Daten ausschließlich zum Wohle der Allgemeinheit genutzt werden sollten, konnte in diesem Fall gegen die Nutzungsbedingungen des Unternehmens verstoßen werden. Um dem öffentlichen Interesse gerecht zu werden, müssen Forschende außerdem ihre Entscheidungen transparent in der Öffentlichkeit diskutieren.[21] Nur so ist die Öffentlichkeit in der Lage, ethische Debatten über das Tun der Wissenschaft zu führen, und nur so können die Meinungen

17 Salganik, *Bit by Bit. Social Research in the Digital Age*, 298.
18 Salganik, *Bit by Bit. Social Research in the Digital Age*, 298; NESH*A Guide to Internet Research Ethics*, 5–6; British Psychological Society, *Ethics Guidelines for Internet-mediated Research* (2017), 17, www.bps.org.uk/publications/policy-and-guidelines/research-guidelines-policy-documents/research-guidelines-poli.
19 Salganik, *Bit by Bit. Social Research in the Digital Age*, 300.
20 „Facebook to researchers: Stop using our data", 2020, https://edition.cnn.com/2020/10/24/tech/facebook-nyu-political-ad-data/index.html.
21 Salganik, *Bit by Bit. Social Research in the Digital Age*, 300–01.

aus solchen Debatten in die Forschungsdesigns einfließen. Hierdurch werden Forschungsprojekte nicht nur verantwortlicher, sondern auch inhaltlich zielgerichteter. *Transparenz* bezieht sich sowohl auf die Offenlegung und Erläuterung des Forschungsprojekts gegenüber den Teilnehmenden als auch auf die Offenheit über die Methoden der Datenerhebung und -verarbeitung bei der Präsentation oder Veröffentlichung von Forschungsergebnissen.

Ethische Grundsätze in Bezug auf die Forschenden selbst

An jedem Forschungsprozesses sind selbstverständlich Forschende beteiligt – ihr Wohlergehen muss sowohl für jedes akademische als auch für das institutionelle Umfeld ein Anliegen sein. Dies bezieht sich auf die *Sicherheit vor Risiken und Gefährdungen der Forschenden*. Insbesondere bei derart sensiblen Themen wie Radikalisierung muss die Forschung so gestaltet werden, dass die Forschenden selbst geschützt werden. Zu den Gefahren könnten physische Bedrohungen und Einschüchterungen durch andere gehören; aber die Sicherheit von Forschenden sollte auch psychologische Unterstützung beinhalten, denn es gibt Grenzen, jenseits derer der Umgang mit den potenziell erschütternden Inhalten, die analysiert werden müssen, gesundheitliche Folgen haben kann. Diese Aspekte gilt es vor Projektbeginn zu berücksichtigen, aber sie werden allzu oft vergessen oder von den an der Forschung beteiligten Institutionen nicht vollumfänglich gewährleistet.

Ein weiteres Thema ist *Vertrauenswürdigkeit*, sowohl aus der Perspektive der Forschungssubjekte als auch der Forschenden. Zum Beispiel müssen die Forschenden hinterfragen, ob ein Online-Profil wirklich echt ist. Die Verifizierbarkeit hat Grenzen, ebenso wie die Transparenz der eigenen Identität. (Aus Sicherheitserwägungen kann es notwendig sein, die eigene Identität zu verbergen.) Viele Nutzer verwenden fiktive Namen, geben falsche Standortinformationen an oder wählen andere Sprachen. Beiträge werden häufig in englischer Sprache verfasst, was eine Erkennung der Nationalitäten der Nutzer schwierig macht.

Außerdem sind Plattformverlagerungen, bei denen ein Thread auf einer Plattform mit einem Thread auf einer anderen Plattform verknüpft wird, eine Herausforderung für Forschende. Abkürzungen, Neologismen, die Vermischung verschiedener Sprachen und unvollständiger Satzbau sind charakteristisch für die Internetkonversation und eine zusätzliche Hürde für die Forschung.[22] Die automatisierte Inhaltsanalyse durch Programme ist hierdurch erschwert und bringt zudem eigenen Herausforderungen mit.[23] Eine Möglichkeit, mit diesen Erschwernissen umzugehen, ist die eingebettete Forschung (embedded research). Ob die forschende Person während des Datenerhebungsprozesses eine aktive oder passive Rolle einnimmt, hat signifikante Auswirkungen auf die interne Validität eines Forschungsdesigns und wirft eine Untermenge ethischer Fragen auf. Wenn es der forschenden Person

22 Albert Bifet and Eibe Frank, „Sentiment knowledge discovery in Twitter streaming data“, in *Discovery Science*, Hrsg. Bernhard Pfahringer, Geoff Holmes und Achim Hoffmann, Lecture Notes in Computer Science (Heidelberg: Springer VS, 2010); Simon Carter, Wouter Weerkamp und Manos Tsagkias, „Microblog language identification. Overcoming the limitations of short, unedited and idiomatic text“, *Language Resources and Evaluation* 47, Nr. 1 (2013).

23 Siehe Alrhmoun, Maher und Winter, *Hass decodieren: Klassifizierung terroristischer Inhalte mittels experimenteller Textanalyse*.

gelingt, bei der Datenerhebung stets eine vollständig passive/beobachtende Rolle einzunehmen, wird sie den beobachteten Kommunikationsprozess vermutlich nicht beeinflussen. Dies kann für die Validität der Forschungsergebnisse von größter Bedeutung sein. Allerdings sind der Beobachtung oft Grenzen gesetzt (z. B. durch gezielte Fragen an das Profil der forschenden Person). Die Grenze zwischen nicht-intrusiver und intrusiver Beobachtung ist ein schmaler Grat.

Aus ethischer Sicht sind auch die Datenschutzeinstellungen relevant für die Durchführung eines Forschungsprojekts. Wenn die gewählten Einstellungen den Content öffentlich einsehbar machen, wird die Analyse dieser Daten durch die Forschung als ein weniger erheblicher Eingriff in die Privatsphäre des Probanden angesehen, als wenn der Content nur für „Freunde“ oder eine noch kleinere, durch den Nutzer definierte Untergruppe ausgewählter Personen bestimmt ist. Zu den ethischen Fragen, die sich bei der Forschung mit Daten aus sozialen Medien stellen, gesellen sich juristische Aspekte. Da mögliche Schäden weder vollständig vermieden noch umfassend antizipiert werden können, ist es das Ziel sowohl der ethischen Reflexion als auch der gesetzlichen Vorschriften, ein ausgewogenes Verhältnis zwischen dem zu erwartenden Nutzen der Forschung und den Datenschutzinteressen herzustellen.[24] Auch wenn rechtliche Anforderungen und ethische Erwägungen voneinander abhängig sind und nur in Kombination verstanden werden können, müssen Forschende beide getrennt behandeln. Im Folgenden gehen wir auf rechtliche Empfehlungen ein, die wir aus der Literatur entnommen haben.

24 Anne Lauber-Rönsberg, „Data Protection Laws, Research Ethics and Social Sciences“, in *Research Ethics in the Digital Age. Ethics for the Social Sciences and Humanities in Times of Mediatization and Digitization*, Hrsg. Farina M. Dobrick, Jana Fischer und Lutz M. Hagen (Wiesbaden: Springer VS, 2018), 41.

3 Zentrale Datenschutzgrundsätze – rechtliche Grenzen, Herausforderungen und Chancen für Forschende

In sozialen Medien im Allgemeinen, aber insbesondere in sozialen Netzwerken, geben Einzelpersonen (und Gruppen) oft sehr viele Informationen über sich preis. Eingestellt werden persönliche Informationen wie ethnische Herkunft, politische Meinungen, religiöse und weltanschauliche Überzeugungen, Sexualleben, sexuelle Orientierung, gesundheitlicher Zustand und Zugehörigkeiten wie z. B. die Mitgliedschaft in einer Gewerkschaft. Einige dieser persönlichen Informationen können für Forschende, die Studien in verschiedenen Bereichen durchführen, von Interesse sein. In welchem Zusammenhang auch immer personenbezogene Daten erhoben oder verwendet werden sollen, in jedem Fall sind die Datenschutzbestimmungen zu beachten. Im Folgenden geben wir einen Überblick über den datenschutzrechtlichen Rahmen der beobachtenden, empirischen Sozialforschung in sozialen Medien auf der Grundlage der Datenschutzgrundverordnung (DSGVO).[25]

Obwohl die Verordnung einige wichtige Privilegien für die wissenschaftliche Forschung enthält, gibt sie keine besonderen Gründe für die Verarbeitung vor. Die Rechtmäßigkeit der Verarbeitung zu Forschungszwecken wird häufig auf der Grundlage einer Interessenabwägung im Einzelfall beurteilt. Bestimmte personenbezogene Daten sind besonders sensibel und unterliegen daher einem erhöhten Schutz (beispielsweise religiöse Überzeugungen oder politische Ansichten, die für die Untersuchung extremistischer Inhalte auf Social-Media-Plattformen von hoher Relevanz sind). Je nach Forschungsprojekt können Forschende auf Grenzen, Herausforderungen und Chancen stoßen, die im Folgenden erörtert werden. Da dies maßgeblich ist, wird hierbei danach unterschieden, ob eine Einwilligung eingeholt wurde oder nicht.

Gesetzliche Regelungen zur Forschung mit personenbezogenen Daten mit Einwilligung der Betroffenen

Viele der in sozialen Medien verfügbaren Daten sind personenbezogen. Auch wenn diese Informationen ohne nennenswerte Hürden online abrufbar sind und von den betroffenen Personen absichtlich gepostet wurden, sind sie als personenbezogene Daten durch die DSGVO

25 Die DSGVO gilt seit dem 25. Mai 2018 in allen Mitgliedsstaaten der EU. Ihr Ziel ist die europaweite Harmonisierung des Datenschutzrechts.

geschützt. Die Erfassung und Auswertung personenbezogener Daten ist für viele Forschungsprojekte unabdingbar. In der Europäischen Union ist der rechtliche Schutz für solche persönlichen Informationen in der Verordnung festgelegt.[26] Da die DSGVO für die Verarbeitung personenbezogener Daten zu Zwecken der wissenschaftlichen Forschung keine spezielle Erlaubnis vorsieht, richtet sich die Zulässigkeit der Datenverarbeitung insbesondere nach den Artikeln 5, 6 und 9. Nach der DSGVO ist die Verarbeitung personenbezogener Daten generell verboten, es sei denn, sie ist unter den gegebenen Umständen ausdrücklich gesetzlich erlaubt oder es liegt eine Einwilligung der betroffenen Person vor.

Durch Erteilung oder Verweigerung der Einwilligung kann eine Person über die Weitergabe und Verwendung ihrer personenbezogenen Daten entscheiden. Ihr muss in jedem Einzelfall die Gelegenheit gegeben werden zu entscheiden, ob und unter welchen Bedingungen ihre Daten verarbeitet werden dürfen. Um dies zu gewährleisten, geben die datenschutzrechtlichen Vorschriften für die Einwilligung in die Verarbeitung personenbezogener Daten bestimmte inhaltliche und formale Anforderungen an die Einwilligung vor. Nach der DSGVO sind dies insbesondere die konkrete Nennung des Verwendungszwecks der Daten, die ausreichende Information der betroffenen Person über die beabsichtigte Verarbeitung ihrer Daten, die Freiwilligkeit der Einwilligung und die Möglichkeit des Widerrufs der Einwilligung zu jedem Zeitpunkt des Forschungsprozesses.

Neben der erklärten Einwilligung einer Person ist die Verwendung durch Forschende auch dann legitimiert, wenn die betroffene Person die sensiblen Daten bewusst öffentlich bereitstellt. In diesen Fällen hebt Artikel 9 (2) (e) der Verordnung das Verarbeitungsverbot nach Absatz 1 auf und die betroffene Person hat kein besonderes Schutzbedürfnis. Die bewusste Veröffentlichung der Daten durch die betroffene Person kann als eine Art Verzicht auf den besonderen Schutz durch Artikel 9 gesehen werden. Doch auch bei bewusster Veröffentlichung durch die betroffene Person entziehen sich die Daten nicht vollständig dem Schutz der DSGVO.[27] Insbesondere gilt Artikel 6 und die Daten benötigen weiterhin eine Rechtsgrundlage für die Verarbeitung, auch wenn Artikel 9 (1) nicht greift.[28]

Hieraus ergibt sich die Frage: was ist mit Daten gemeint, die „öffentlich gemacht“ wurden”? Daten gelten als öffentlich, wenn sie einer unbestimmten Anzahl von Personen ohne nennenswerte Zugangshürde zugänglich gemacht werden. Ein weiterer zentraler Aspekt bezüglich der Anforderungen des Datenschutzes ist daher die Art der sozialen Medien, aus denen die Daten stammen. Stammen sie aus offenen oder geschlossenen (Teilen von) sozialen Medien oder aus sozialen Medien, die speziell für Forschungszwecke eingerichtet wurden? Das primäre Abgrenzungskriterium ist hier die „Zugangshürde durch Registrierung und Login“.[29] Je nach Plattform haben Nutzer die Möglichkeit, die Gruppe der Adressaten ihrer Inhalte einzuschränken. Bestimmte soziale Medien sind speziell für Forschungszwecke eingerichtet, wobei sich

26 Der Anwendungsbereich der Verordnung umfasst alle Arten und Formen der „Verarbeitung“ von Daten und damit die Erhebung, Speicherung, Strukturierung usw. Siehe Artikel 4 (2) DSGVO.
27 Golla, Hofmann und Bäcker, „Connecting the Dots: Sozialwissenschaftliche Forschung in Sozialen Online-Medien im Lichte von DS-GVO und BDSG-neu“ 92.
28 An dieser Stelle sei darauf hingewiesen, dass Artikel 6 DSGVO gleichzeitig mit Artikel 9 DSGVO anwendbar ist. Beide stehen dann nebeneinander und müssen beide erfüllt werden.
29 Golla, Hofmann und Bäcker, „Connecting the Dots: Sozialwissenschaftliche Forschung in Sozialen Online-Medien im Lichte von DS-GVO und BDSG-neu“, 96.

die Einwilligung der Nutzer in die Verarbeitung personenbezogener Daten als praktikable Lösung erweist. Dies ist bei anderen sozialen Medien nicht der Fall. Damit werden die gesetzlichen Anforderungen an die Verarbeitung von personenbezogenen Daten relevant. Dies gilt auch dann, wenn die erhobenen Daten aus öffentlich zugänglichen Quellen stammen.[30] Außerdem können „öffentliche Informationen in den Bereich des Privatlebens fallen, wenn sie systematisch gesammelt und in Dateien der Behörden gespeichert werden".[31] Darüber hinaus haben Einzelpersonen auch dann ein Recht auf Privatsphäre, wenn sie sich freiwillig in die Öffentlichkeit begeben. Daten aus halböffentlichen oder gar geschlossenen Kommunikationsräumen sind noch schutzbedürftiger als Daten aus öffentlichen Räumen.

Wie bereits erwähnt, kann die Einholung der Zustimmung jedoch oft die Forschung selbst gefährden, oder sie ist aufgrund der großen Anzahl von Personen, deren Zustimmung eingeholt werden müsste, schlichtweg unmöglich. Dies ist nicht nur bei der Forschung zu radikalisierten oder extremistischen Personen oder Kollektiven der Fall, sondern auch in vielen anderen sensiblen Forschungsbereichen. Aus diesem Grund wenden wir uns im Folgenden den gesetzlichen Regelungen für die Forschung mit personenbezogenen Daten ohne Einwilligung der betroffenen Personen zu.

Gesetzliche Regelungen zur Forschung mit personenbezogenen Daten ohne Einwilligung der Betroffenen

Da die Forschung zur Erreichung der Forschungsziele vielfach auf personenbezogene Daten angewiesen ist, hat der Gesetzgeber Zulässigkeitskriterien für die Forschung festgelegt. Hiermit kann das Recht auf informationelle Selbstbestimmung zum Zwecke der wissenschaftlichen Forschung eingeschränkt werden. Wenn eine Untersuchung Daten verwendet, die nicht in die speziellen Kategorien von Artikel 9 der DSGVO fallen, richtet sich die Rechtmäßigkeit ihrer Verarbeitung stattdessen ausschließlich nach Artikel 6. Dementsprechend muss bei der Verarbeitung personenbezogener Daten mindestens eine der in diesem Artikel genannten Bedingungen erfüllt sein. Folglich ist die Verarbeitung personenbezogener Daten ohne Einwilligung nur unter ganz bestimmten Umständen zulässig: beispielsweise wenn entweder die schutzwürdigen Interessen der betroffenen Person in keiner Weise beeinträchtigt werden oder das öffentliche Interesse an der Durchführung des Forschungsvorhabens die schutzwürdigen Interessen der betroffenen Person überwiegt und der Forschungszweck auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann. Wenn eine derartige Bedingung gegeben ist, kann die Forschung ohne die Zustimmung der betroffenen Person(en) durchgeführt werden. Die Rechtmäßigkeit der Verarbeitung ohne Einwilligung hängt oft von einer Abwägung zwischen dem Recht auf Privatsphäre und

30 Ian Brown und Josh Cowls, *Check the Web. Assessing the Ethics and Politics of Policing the Internet for Extremist Material*, Oxford Internet Institute (2015), 46. Öffentliche Räume zeichnen sich durch einen ungehinderten Zugang mit der Kopräsenz von Fremden aus. Im Gegensatz dazu „sind private Räume durch eingeschränkten Zugang ... und die Abwesenheit von Fremden charakterisiert" Nicolas Legewie und Anne Nassauer, „YouTube, Google, Facebook: 21st Century Online Video Research and Research Ethics", *Forum: Qualitative Social Research* 19, 32, Nr. 3 (2018).

31 Antrag beim Europäischen Gerichtshof für Menschenrechte, „Rotaru vs. Rumänien Nr. 28341/95", (2000): § 43.

dem Nutzen der Forschung ab. In jedem Fall ist eine Abwägung zwischen dem Forschungsinteresse und den berechtigten Interessen der betroffenen Person erforderlich.

Für die Verarbeitung besonderer Kategorien personenbezogener Daten zu Forschungszwecken gibt es gemäß Art. 9 (2) (j) der DSGVO ebenfalls gesetzliche Regelungen: Erstens, das Vorhandensein einer *konkreten Forschungsfrage und eines entsprechenden Konzepts*. Für wissenschaftliche Forschungszwecke muss die forschende Person nachweisen, dass das jeweilige Forschungsvorhaben in seiner Struktur und seinem Inhalt wissenschaftlichen Anforderungen genügt. Zweitens müssen Forschende *die Undurchführbarkeit des Projekts* ohne die konkreten personenbezogenen Daten nachweisen. Sie müssen daher ausführlich darlegen, warum die Erhebung der entsprechenden personenbezogenen Daten für das Forschungsprojekt dringend erforderlich ist. Forschende sollten sich also fragen, ob die Studie auch mit weniger Daten oder mit anderen Arten von Daten durchgeführt werden kann. Drittens müssen wieder Interessen abgewogen werden, wie zum Beispiel die Menge der Daten und die besonderen Umstände der Betroffenen. Um eine Datenverarbeitung zu Forschungszwecken ohne Einwilligung der betroffenen Person zu legitimieren, muss also dargelegt werden, warum das Forschungsinteresse das Interesse der betroffenen Person am Schutz ihrer Daten (deutlich) überwiegt.

Dazu sind die *Grundsätze der Notwendigkeit, der Angemessenheit und der Verhältnismäßigkeit* der Verarbeitung personenbezogener Daten zu beachten und Zugriffsregelungen zu treffen, die eine datenschutzkonforme Verwendung personenbezogener Daten sicherstellen: Zunächst müssen die Forschenden nachweisen, dass das Projekt einen *legitimen Zweck* verfolgt. Es stimmt zwar, dass Forschung generell als legitimer Zweck angesehen werden kann,[32] doch sollte die Verarbeitung personenbezogener Daten für ein Forschungsprojekt ohne die Einwilligung der Betroffenen nur dann in Betracht gezogen werden, wenn der Forschungszweck nicht auf anderem Wege erreicht werden kann.[33] *Notwendigkeit* ist als eine weitere Voraussetzung für die Verhältnismäßigkeit zu verstehen. Eine Maßnahme ist notwendig, wenn keine sanftere – d. h. weniger stark in die Privatsphäre eindringende – Maßnahme dasselbe Ziel erreichen kann. Die Notwendigkeitsprüfung sollte als erster Schritt gelten, den ein vorgeschlagenes Vorhaben, das die Verarbeitung personenbezogener Daten beinhaltet, absolvieren muss. Sollte das jeweilige Vorhaben der Notwendigkeitsprüfung nicht standhalten, ist eine Prüfung der Verhältnismäßigkeit nicht mehr erforderlich. Ein Vorhaben, das sich als nicht notwendig erweist, ist so zu modifizieren, dass es den Kriterien der Notwendigkeit entspricht.

Die Verarbeitung von online gewonnenen Daten ohne Einwilligung der betroffenen Person muss auch das Kriterium der *Angemessenheit* erfüllen. Der Grundsatz der Angemessenheit verlangt, dass Inhalt und Form des Vorhabens das zur Zielerreichung notwendige Maß nicht überschreiten. Um die Angemessenheit des Eingriffs in die Privatsphäre zu prüfen, müssen Forschende die gesetzliche Rechtfertigung für diesen Eingriff (oftmals basierend auf dem wahrgenommenen gesellschaftlichen Nutzen der Forschung) gegen die Verpflichtung

32 Golla, Hofmann und Bäcker, „Connecting the Dots: Sozialwissenschaftliche Forschung in Sozialen Online-Medien im Lichte von DS-GVO und BDSG-neu", 90.
33 Sold, Abay Gaspar und Junk, Designing Research on Radicalisation using Social Media Content: Data Protection Regulations as Challenges and Opportunities, 62–63.

zum Schutz der Person, deren Privatsphäre durch den Eingriff verletzt wird, abwägen. Nach dieser Prüfung müssen Forschende zudem nachweisen, dass gemäß Artikel 89 der DSGVO Maßnahmen und Garantien zum Schutz der betroffenen Personen, wie beispielsweise Pseudonymisierung, eingehalten werden.

Ein weiterer relevanter Aspekt bei der Betrachtung des Forschungsprojekts aus der Perspektive des Datenschutzes betrifft die Aktivität bzw. Passivität des Forschenden. Die Frage, ob die Forschenden bei der Datenerhebung passive Beobachter sind – also eine nicht-reaktive Erhebungsmethode gewählt haben – hat ebenfalls Auswirkungen auf die Datenschutzanforderungen. Bei einem solchen Verfahren nimmt die forschende Person zu keinem Zeitpunkt eine aktive Rolle ein und tritt nicht in den Diskurs ein. Zwar schließt eine solche passive Beobachtung auch das Einholen einer Einwilligung von vornherein aus,[34] doch hält sich der Eingriff insofern in Grenzen, als kein Einfluss darauf genommen wird, was kommentiert oder gepostet wird. Demgegenüber bedeutet aktive Forschung zwar, dass es möglich ist, die Zustimmung zur Erfassung und Analyse personenbezogener Daten einzuholen. Sie birgt aber auch das Risiko, störenden Content zu produzieren, den Diskurs (weiter) voranzutreiben oder unter Umständen das Postingverhalten anderer zu beeinflussen.

Personen, deren Zustimmung nicht eingeholt werden kann, sollte weiterer Schutz geboten werden. Nach Artikel 89 (1) der DSGVO sind technische und organisatorische Maßnahmen zu treffen, die insbesondere die Achtung des Grundsatzes der Datenminimierung gewährleisten. Wichtige Aspekte sind in diesem Zusammenhang die Reduzierung der Menge der erhobenen Daten und die Beschränkung des Umfangs der Verarbeitung nur auf das für den Zweck notwendige Maß, die Festlegung einer Speicherfrist sowie eine Regelung zur Zugänglichkeit der Daten. Soweit die verfolgten Zwecke auch mit anonymisierten oder pseudonymisierten Daten erreicht werden können, müssen nach Artikel 89 (1), Satz 3 und 4 DSGVO anonymisierte oder pseudonymisierte Daten verwendet werden. Was die Datenarchivierung betrifft, so liegt die Notwendigkeit von Rollenkonzepten und sicheren Zugriffslösungen auf der Hand.[35]

Darüber hinaus müssen auch dann, wenn personenbezogene Daten (aufgrund einer Einwilligung oder einer gesetzlichen Bestimmung) verarbeitet werden dürfen, technische und organisatorische Maßnahmen getroffen werden, die die Erfüllung der Zwecke des Datenschutzes sicherstellen. Dies kann zum Beispiel durch die getrennte Speicherung von Identifikatoren und Daten erreicht werden. Des Weiteren sollten die Daten für einen bestimmten Zweck gekennzeichnet werden. Informationen werden daher nur für den Zweck, für den sie erhoben wurden, gespeichert und untersucht.

34 Kerstin Eppert et al., *Navigating a Rugged Coastline: Ethics in Empirical (De-)Radicalization Research*, core-nrw Netzwerk für Extremismusforschung in Nordrhein-Westfalen (Bonn, 2020), 9, https://www.bicc.de/fileadmin/Dateien/Publications/other_publications/Core-Forschungsbericht_1/CoRE_FP_1_2020.pdf.

35 Golla, Hofmann und Bäcker, „Connecting the Dots: Sozialwissenschaftliche Forschung in Sozialen Online-Medien im Lichte von DS-GVO und BDSG-neu“, 94.

4 Datenquelle, Plattform-richtlinien und Forschende – Überblick, Zusammen-wirken und Empfehlungen

Neben ethischen Grundsätzen und datenschutzrechtlichen Vorschriften müssen Nutzer und Forschende bei der Nutzung von Fremdprogrammen die rechtlichen Vereinbarungen mit der jeweiligen Plattform sowie weitere individuelle Einschränkungen beachten. Dass die führenden Plattformen unterschiedliche Nutzungsbedingungen verwenden, die oft auch noch lang oder schwer zu verstehen sind, ist eine Herausforderung für sich. Im Folgenden geben wir einen kurzen Überblick über die wichtigsten Bedingungen führender Technologieunternehmen und leiten einige allgemeine Empfehlungen ab.

Twitter

Mit der neuen Datenschutzrichtlinie von Twitter, die im Einklang mit der DSGVO steht und im Mai 2018 in Kraft trat, gibt Twitter seinen Nutzern mehr Kontrolle über ihre Daten. Da sie unabhängig vom Zugriffsort für alle Nutzer gilt, scheint der Schutz der DSGVO auf alle Nutzer rund um den Globus ausgeweitet zu werden. Twitter erfasst Informationen zur IP-Adresse und zum Gerätetyp von Nutzern, sobald diese sich Tweets ansehen. Natürlich werden auch Daten generiert und erfasst, wenn ein Nutzer Tweets sendet, mit anderen Nutzern interagiert, retweetet, likt usw. Gemäß der Datenschutzerklärung von Twitter sind Inhalte von Direktnachrichten von der Datenerfassung und -verarbeitung ausgenommen. Die erfassten Daten werden verwendet, um Tweets zu empfehlen, Accounts zu verfolgen und gezielte Werbung zu platzieren. Bis zu einem gewissen Grad bietet Twitter seinen Nutzern die Kontrolle darüber, welche Arten von Daten erfasst werden dürfen. So können die Nutzer beispielsweise ihre Accounts auf öffentlich oder privat einstellen und das Taggen von Fotos durch andere ein- oder ausschalten. Darüber hinaus kann der Nutzer Informationen herunterladen, die der Nutzer auf Twitter geteilt hat. So werden den Nutzern neben den öffentlichen Tweets, die „sofort für jeden weltweit sichtbar und auffindbar sind“, auch „nichtöffentliche Wege der Kommunikation über geschützte Tweets und Direktnachrichten“ zur Verfügung gestellt.[36] Zusätzlich ist es möglich, Twitter mit einem Pseudonym zu nutzen, und „Daten werden maximal 18 Monate lang oder bis zur Löschung des Accounts aufbewahrt“.[37] Mit der Einführung seines API v2 im August 2020 „macht Twitter es Unternehmen, Forschenden und Third-Party-Entwicklern einfacher, auf seiner

36 Twitter, *Twitter Privacy Policy* (2020), https://cdn.cms-twdigitalassets.com/content/dam/legal-twitter/site-assets/privacy-june-18th-2020/Twitter_Privacy_Policy_EN.pdf.
37 Identity Guard, „What You Need to Know About Twitter's Privacy Policy“, (2018), https://www.identityguard.com/news/twitter-privacy-policy.

Plattform aufzubauen“:[38] Es bietet Third-Party-Entwicklern Zugang zu Funktionen, die ihren Clients lange Zeit fehlten, unter anderem „Threads, Umfrageergebnisse in Tweets, an Profilseiten angeheftete Tweets, Spam-Filter sowie eine leistungsfähigere Stream-Filterung und Suchanfragesprache“.[39] Darüber hinaus besteht Zugriff auf einen Echtzeit-Stream von Tweets.

Twitter hat den API-Zugang auf drei Ebenen neu organisiert: Während der Early-Access-Periode war es möglich, „das öffentliche Gespräch mitzuhören und zu analysieren“.[40] Da jedoch nur die kostenlose, elementare Access-Ebene eingeführt wurde, die die Anzahl der API-Aufrufe für Entwickler begrenzt, bleibt abzuwarten, welche Änderungen und Möglichkeiten sich für Forschende ergeben werden. Ein wichtiger Vorteil von Twitter im Vergleich zu anderen sozialen Netzwerken ist die offene Kommunikation. Einzelne Tweets oder ganze Unterhaltungen können durch jeden gesucht und gelesen werden, unabhängig davon, ob man selbst Nutzer ist oder sich gegenseitig auf Twitter folgt. So haben Forschende nicht nur Zugriff auf umfassende und ungefilterte Daten, sondern müssen auch keine besonderen Datenschutzauflagen einhalten. Eine Einschränkung bei der Twitter-Forschung ist, dass die Datennutzung den wirtschaftlichen Interessen von Twitter nicht schaden darf. Die Erstellung, Anreicherung und Verbreitung von großen Datenbanken mit Tweets ist verboten, auch für nicht-kommerzielle Zwecke.[41] Resultate können nicht gewichtet oder verglichen werden, da Forschende keine Informationen über die gesamte Twitter-Aktivität haben.

Facebook

Ähnlich wie Twitter hat auch Facebook seine Datenschutzrichtlinien nicht nur entsprechend der DSGVO überarbeitet, sondern auch für seine Kunden weltweit anwendbar gemacht. Facebook, Instagram, Messenger und andere von Facebook angebotene Produkte und Funktionen sammeln verschiedene Arten von Informationen, abhängig von den Interaktionen der Nutzer mit Facebook-Produkten. Dazu gehören Informationen und hochgeladene Inhalte, Daten der sozialen Netzwerke des Nutzers (wie die Accounts, Gruppen, Hashtags usw., mit denen er interagiert), Nutzungsinformationen und Daten zu plattforminternen Käufen sowie Daten zu Interaktionen anderer Nutzer mit den Inhalten und Profilen eines Nutzers. Darüber hinaus werden Daten über Geräte gesammelt, die mit Facebook oder Instagram verbunden sind, einschließlich Geräteattribute, Cursorbewegungen, Internetanbieter, Telefongesellschaften und Geräteeinstellungen. Facebook nutzt diese Daten, um die eigenen Produkte zu verbessern und Inhalte und Account-Empfehlungen individuell anzupassen. Außerdem stellt Facebook die Daten Third-Party-Kunden zur Verfügung. Dabei werden Daten nicht nur mit Werbetreibenden geteilt, sondern auch mit Dritten, die Apps auf Facebook betreiben oder die Dienste von Facebook anderweitig nutzen. Wie bei anderen Social-Media-Plattformen können Nutzer die Datenerfassung mit

38 „Twitter launches new API as it tries to make amends with third-party developers“, 2020, https://www.theverge.com/2020/8/12/21364644/twitter-api-v2-new-access-tiers-developer-portal-support-developers.
39 „Twitter ändert API zugunsten von Third-Party-Entwicklern“ 2020, https://onlinemarketing.de/technologie/twitter-api-third-party-entwicklern.
40 „Twitter API v2: Early Access“, 2020, https://developer.twitter.com/en/docs/twitter-api/early-access.
41 Michael Beurskens, „Legal questions of Twitter research. Twitter and society“, in *Digital Formations*, Hrsg. Katrin Weller (New York et al.: Peter Lang, 2014).

ihren Einstellungen einschränken sowie die über sie gesammelten Nutzerdaten per Download abrufen. Bestimmte Daten unterliegen einem besonderen Schutz: Nutzer können Facebook freiwillig Informationen über ihre religiösen oder politischen Ansichten, ihren Gesundheitszustand, ihre ethnische Herkunft oder Volkszugehörigkeit, ihre philosophischen Überzeugungen oder ihre Mitgliedschaft in einer Gewerkschaft zur Verfügung stellen.[42] Obwohl Facebook in letzter Zeit einige Verbesserungen in Bezug auf den Schutz der Privatsphäre vorgenommen hat,[43] ist die Benutzeroberfläche nach wie vor nicht transparent genug. Außerdem können Nutzer, im Gegensatz zur personalisierten Werbung, die Datensammlung kaum einschränken. Facebook gibt seinen Nutzern die Möglichkeit, über das so genannte „Zugriff auf deine Informationen"-Werkzeug ihre Facebook-Daten abzurufen, unter anderem Fotos, Beiträge, Reaktionen und Kommentare. Außerdem können Nutzer mit „Deine Informationen herunterladen" eine Kopie ihrer Facebook-Informationen herunterladen.

Facebook stellt zudem Forschung und Wissenschaft Informationen und Inhalte für die Durchführung von Untersuchungen zur Verfügung.[44] Als Reaktion auf das Cambridge-Analytica-Debakel im Jahr 2018 versprach Facebook eine Forschungsinitiative, um der Wissenschaft Zugang zu Facebook-Daten zu gewähren, während die Nutzerinformationen privat bleiben. Trotz der Einführung eines neuen Datenzugriffscenters (data access hub), über das Forschende alle für sie verfügbaren Facebook-Datensätze einsehen können, wird Facebook weiterhin dafür kritisiert[45], dass es Forschende nicht ausreichend unterstütze.

Google

Google scheint im Gegensatz zu Facebook und Twitter bisher davon abgesehen zu haben, seine überarbeitete Datenschutzrichtlinie, die im Einklang mit der DSGVO steht, auf Regionen außerhalb der EU anzuwenden. So wurde beispielsweise berichtet, dass Nutzer in Großbritannien den Schutz durch die EU-DSGVO verlieren und nach dem Brexit nun akzeptieren müssen, dass ihre Daten, anders als in der EU, wo sie auf Servern gemäß den DSGVO-Regeln gespeichert werden müssen, in den USA gespeichert werden. Das bedeutet, dass das Datenschutzniveau entsprechend den Richtlinien variiert, die die Dienstanbieter weitestgehend selbst festlegen. Selbst YouTube ist nur ein Teil des Google-Imperiums, das aus Dutzenden von Apps, Diensten und einem mobilen Betriebssystem besteht. Das Unternehmen sammelt daher mit großer Wahrscheinlichkeit mehr Daten über seine Nutzer als beispielsweise Twitter oder Facebook. YouTube erfasst unter anderem Daten über Nutzerinteraktionen, Kommentare, Video-Uploads, Videokonsum und vieles mehr. YouTube gibt zwar Nutzerdaten an Dritte weiter, die auf der Plattform Werbung schalten, und stellt eine API zur Verfügung. Es wird jedoch ausdrücklich darauf hingewiesen, dass YouTube keine Daten an Dritte verkauft, wie zum Beispiel andere Social-Media-Unternehmen.

42 „Data Policy", 2020, https://www.facebook.com/policy.php.
43 „Mit mehr Kontrolle über die eigene Privatsphäre ins neue Jahrzehnt", 2020, https://about.fb.com/de/news/2020/01/mehr-kontrolle-uber-die-eigene-privatsphare/.
44 Ausführlichere Informationen siehe „Facebook Research. Supporting exciting and innovative research through meaningful engagements", 2020.
45 Siehe z. B. „Facebook needs to share more with researchers", World View, 2020, https://www.nature.com/articles/d41586-020-00828-5.

YouTube bietet Nutzern, die auf ihre Daten zugreifen möchten, zahlreiche Möglichkeiten, die Daten zu überprüfen und sogar zu löschen.

TikTok

Im Gegensatz zu vielen großen Social-Media-Unternehmen verfolgt TikTok je nach Region unterschiedliche Datenschutzansätze. In Europa gibt es zum Beispiel eine Richtlinie, die bestimmte Anforderungen der DSGVO berücksichtigt. Für die USA und andere Länder gelten gesonderte Richtlinien. Neben den üblichen Datenpunkten (Nutzungsaktivitäten, Geräteinformationen, Standortdaten, Telefonbuch bei Zugriff, Informationen zu auf der Plattform geteilten Inhalten Dritter) werden auch Inhalte gesammelt und analysiert. TikTok bietet Forschenden offenbar keinen Zugang zu einem API oder anderen Mitteln zur legalen Datenerfassung. Stattdessen haben IT-Spezialisten Möglichkeiten gefunden, inoffizielle APIs zu erstellen, um Daten über Nutzer, Aufrufe und Interaktionen zu sammeln.[46]

Telegram

Ähnlich wie TikTok hat auch Telegram eine eigene Datenschutzrichtlinie für europäische Nutzer. Als Kommunikationsplattform speichert Telegram nur grundlegende Informationen über seine Nutzer (Telefonnummer, E-Mail-Adresse, Benutzername usw). Regelmäßige Chats („Cloud-Chats“) zwischen Nutzern und Gruppenchats werden ebenfalls gespeichert. Geheime Chats sind den Angaben zufolge vollständig verschlüsselt und nur für die beteiligten Nutzer sichtbar. Auch Telegram stellt Forschenden keine Mittel zum Sammeln und Analysieren von Daten zur Verfügung, wie zum Beispiel ein API. Die Forschung hat jedoch ihren eigenen Scraper erstellt, um zu Forschungszwecken auf öffentliche Kanäle, Interaktionen und Nachrichten zuzugreifen.[47] Zwar ist „Scraping“ (das Auslesen von Bildschirminhalten) ein attraktives Werkzeug für die Auswertung sozialer Netzwerke zu Forschungszwecken, doch stellt es in Bezug auf die Rechtmäßigkeit und ethische Erwägungen eine besonders umstrittene Art der Datenbeschaffung dar.[48]

Allgemeine Empfehlungen

Aus dieser Übersicht ergibt sich bestenfalls ein diffuses Bild: Einige Daten sind für die Forschung verfügbar, je nach Plattform. Generell behalten sich die Plattformen die Rechte an den Daten, an deren Verarbeitung und Weitergabe vor. Allerdings haben nicht alle Plattformen die Zugangspunkte und Bedingungen für die wissenschaftliche Nutzung klar festgelegt. Wünschenswert wäre auch eine weitere Öffnung vieler Technologieunternehmen für die Wissenschaft mit klaren, permanenten und harmonisierten APIs und hinsichtlich der Suche (beispielsweise nach Datensätzen, die mit einem Suchbegriff erstellt werden). Auf Twitter zum Beispiel werden Tweets,

46 „How to Collect Data from TikTok“, 2020, https://towardsdatascience.com/how-to-collect-data-from-tiktok-tutorial-ab848b40d191.
47 Jason Baumgartner et al., *The Pushshift Telegram Dataset* (2020).
48 Sebastian J. Golla und Max von Schönfeld, „Kratzen und Schürfen im Datenmilieu – Web Scraping in sozialen Netzwerken zu wissenschaftlichen Forschungszwecken“, *Kommunikation und Recht* (2019).

die durch Antworten verlinkt sind, nicht in den Suchergebnissen angezeigt. Data Grants[49] ist ein Pilotprogramm, das Forschenden Zugang zu öffentlichen und historischen Daten ermöglicht; allerdings ist dieser Zugang auf wenige, von Twitter ausgewählte, Projekte beschränkt.

Die Erforschung und Untersuchung des oft gewalttätigen politischen Online-Extremismus steht ganz oben auf der Agenda verschiedener politischer und gesellschaftlicher Institutionen sowie der Technologieunternehmen. Datenbanken mit Benutzerdaten unterliegen, wie bereits oben in diesem Bericht erwähnt, den jeweiligen nationalen Datenschutzbestimmungen. Diese schränken aus guten Gründen die Weitergabe vorhandener Daten an andere Forschende im In- und vor allem Ausland ein. In diesem Zusammenhang lohnt es sich zu hinterfragen, wie Forschende die gesammelten Daten für weitere Analysen und Projekte nutzen können. Während die DSGVO für alle EU-Mitgliedsstaaten gilt, sind die Regeln für die Zusammenarbeit mit Partnern außerhalb der EU weniger klar, auch wenn sich die Standards weltweit immer mehr annähern und Technologieunternehmen wie Facebook globale Regeln implementieren und vorantreiben.

Zwar gibt es noch immer eine Vielzahl von Einschränkungen, doch die Tendenz ist vielversprechend. Zudem gibt es in den meisten Datenschutzbestimmungen, und so auch in der DSGVO, bestimmte Privilegien für die Forschung. Wenn bestimmte Prinzipien systematisch und transparent in Datenschutzstrategien für gegebene Forschungsprojekte und in enger Absprache mit den Datenschutzbeauftragten (und ggf. mit den Plattformen) abgewogen werden, sind die notwendigen Auswertungen und der Zugang zu den Ergebnissen für andere Forschende in fast jedem Fall möglich. Dennoch gibt es gewisse Grenzen bei der Reproduzierbarkeit der Ergebnisse, wenn Daten aus verschlüsselten Bereichen und unter der Bedingung der Pseudonymisierung oder Anonymisierung abgerufen werden. Erschwerend kommt hinzu, dass immer mehr extremistische Inhalte schnell wieder gelöscht werden. Wenn gelöschte extremistische Inhalte sicher gehostet würden, könnten Forschende, die Zugang zu solchen Inhalten haben, mutmaßlich eine gründlichere Analyse vornehmen. In dieser Hinsicht gibt es erheblichen Diskussionsbedarf mit akademischen Online- und Print-Verlagen, um beispielsweise ein hohes Maß an externer Validität veröffentlichter Studie zu gewährleisten, ohne Anreize für die Verletzung von Datenschutzbestimmungen und Grundsätzen der Forschungsethik zu schaffen. Wird hier keine Balance gefunden, liefert die Forschung eine viel zu geringe Menge an relevanten Ergebnissen.

Eine enge Kooperation zwischen Technologieunternehmen und Forschung in den Bereichen Wissensaustausch, technische Zusammenarbeit und gemeinsame Forschung ist vorteilhaft für beide Seiten. Forschende könnten beispielsweise in wesentlich größerem Umfang problematische Inhalte melden, müssen sich dabei aber kritisch mit den Auswirkungen des Meldens in Zusammenhang mit den oben umrissenen ethischen Standards auseinandersetzen. Technologieunternehmen müssen ihrerseits die Mechanismen für den Umgang mit gemeldeten Inhalten transparent machen und die ethischen und forschungspraktischen Herausforderungen kennen,

49 Siehe „Introducing Twitter Data Grants“, 2014, https://blog.twitter.com/engineering/en_us/a/2014/introducing-twitter-data-grants.html.

mit denen Forschende in diesem Zusammenhang konfrontiert sind. Eine Lösung könnte die Bereitstellung einer Option sein, um von Forschenden gemeldete Inhalte anders zu behandeln als andere: die Unternehmen könnten solche Inhalte genau überwachen, ohne sie zu löschen. Ein Beispiel für die erfolgreiche Zusammenarbeit zwischen Technologieunternehmen und Forschung ist das Global Internet Forum to Counter Terrorism (GIFCT). Eines der zentralen Ziele des GIFCT ist es, „Forschende zu befähigen, Terrorismus und Terrorismusbekämpfung zu untersuchen, einschließlich der Entwicklung und Evaluierung von Best Practices für die Zusammenarbeit verschiedener Interessengruppen und der Verhinderung des Missbrauchs digitaler Plattformen".[50] GNET wird durch das GIFCT gefördert; die dadurch ermöglichten (sowohl kritischen als auch offenen) Dialoge sind überaus wertvoll und müssen zur Vertiefung auf Dauer fortgesetzt werden.

Es gibt diverse Tools oder zumindest plattformübergreifende Initiativen, die für Forschende, die mit öffentlichen Inhalten aus sozialen Medien arbeiten, von Interesse sind. CrowdTangle[51] ist ein solches Tool, mit dem sich öffentliche Inhalte in sozialen Medien analysieren und zu Berichten zusammenstellen lassen. CrowdTangle macht den Zeitpunkt eines Beitrags, die Art des Beitrags (Video, Bild, Text) und Informationen darüber zugänglich, auf welcher Seite, in welchem öffentlichen Account oder in welcher öffentlichen Gruppe er gepostet wurde und wie viele Interaktionen (z. B. „Gefällt mir"-Angaben, Reaktionen, Kommentare, wie oft der Beitrag geteilt wurde) oder Videoaufrufe er generiert hat sowie welche anderen öffentlichen Seiten oder Accounts ihn geteilt haben. Dies ist zwar ein guter Anfang, aber es gibt noch Spielraum für Verbesserungen und Erweiterungen. An CrowdTangle wird unter anderem kritisiert, dass es für Forschende nicht besonders nützlich ist, da es schwierig ist, nach Mustern zu scannen, die nicht im Voraus bekannt sind.[52] Außerdem benötigen viele Forschungsprojekte gerade nicht öffentliche Daten. Neben CrowdTangle oder einer möglichen Überarbeitung des Angebots sind weitere Initiativen willkommen. Da die Nutzer von einer Plattform zur anderen wechseln, extremistische Netzwerke sich über verschiedene Plattformen erstrecken und Inhalte zunehmend plattformübergreifend gepostet werden, wären übergreifende Tools ein großer Fortschritt für die künftige Forschung. Sie würden weitere Disziplinen und Forschende ins Boot holen, um die verschiedenen gesellschaftlichen und politischen Herausforderungen zu analysieren, die sich aus der Online-Dynamik des Extremismus ergeben: weitere derartige Initiativen sind notwendig und willkommen.

50 „Global Internet Forum to Counter Terrorism: Evolving an Institution", 2020, https://www.gifct.org/about/.
51 Umfassender Zugang zu CrowdTangle ist ausgewählten Unternehmen und Organisationen vorbehalten, die die entsprechenden Anforderungen erfüllen. Die Chrome-Erweiterung CrowdTangle Link Checker steht hingegen allen Interessenten zur Verfügung. Die Erweiterung zeigt an, wie oft eine URL geteilt wurde, welche öffentlichen Seiten oder Accounts die URL geteilt haben, und die Interaktionsdaten für diese Beiträge.
52 Hegelich, „Facebook needs to share more with researchers".

5 Schlussbemerkungen

Manche Forschende vermeiden es immer noch, mit Daten aus sozialen Medien zu arbeiten, oder beginnen Forschungsprojekte, ohne Datenschutzfragen und ethischen Grundsätzen genügend – oder überhaupt – Aufmerksamkeit zu schenken. Um die Zögerlichkeit der Forschenden zu verringern, hat dieser Bericht einen Überblick über die wichtigsten ethischen Überlegungen und Datenschutzanforderungen gegeben, mit denen Forschende bei der Arbeit mit personenbezogenen Daten aus sozialen Medien konfrontiert werden, und die Herausforderungen und Grenzen dieser Art der Arbeit aufgezeigt. Trotz dieser Hürden können und sollten wir die Analyse von Daten aus der digitalen Welt nicht unterlassen, denn Online- und Offline-Welt sind längst eng miteinander verbunden. Um Phänomene besser verstehen zu können, ist eine Betrachtung beider Welten unumgänglich. Unser Ziel ist es daher, andere Forschende zu ermutigen, mit Daten aus sozialen Medien zu arbeiten, und zu diesem Zweck weist der Bericht auch auf die Chancen hin.

Dabei müssen Forschende im Rahmen des Möglichen ihre Pflichten und Verantwortlichkeiten erfüllen und jegliches Risiko für die Forschungssubjekte minimieren. Sie sollten außerdem, wann immer möglich, eine informierte Einwilligung einholen, hochgradig identifizierbare Informationen löschen und Einwilligungsnachweise bis zur Verbreitungsphase eines Projekts aufbewahren. In allen Phasen eines Forschungsprojekts (von Beginn an bis zur Verbreitung der Ergebnisse und bis zum Umgang mit den Daten nach Projektabschluss) sind ethische und datenschutzrechtliche Anforderungen zu berücksichtigen.

Daten von verschiedenen Plattformen sind für Forschende von Interesse. Die Datenschutzrichtlinien der einzelnen Technologieunternehmen sind so unterschiedlich wie die Plattformen selbst. Trotz einiger Überschneidungen – zum Beispiel erfüllen Facebook und Twitter für ihre globalen Nutzer die DSGVO-Anforderungen – gibt es auch Unterschiede, von denen einige im vorliegenden Beitrag erörtert wurden. Obwohl in den vergangenen Jahren mehr Wert auf nutzerfreundliche Grundsätze gelegt wurde, nicht zuletzt aufgrund der gestiegenen Anforderungen und des Drucks auf die Plattformbetreiber, ist es oft unklar, welche Möglichkeiten Forschenden zur Verfügung stehen. Es besteht ein dringender Bedarf an weiteren Verbesserungen hinsichtlich der plattformübergreifenden Rechte und des Zugangs für Forschende. Auch wenn es bereits positive Entwicklungen gibt, müssen die Technologieunternehmen der Forschung weitere Erleichterungen einräumen. Umgekehrt sollte auch die Forschung die bestehenden Angebote der Technologieunternehmen stärker nutzen – im Einklang mit den ethischen und rechtlichen Grundsätzen, die wir in diesem Bericht umrissen haben und die, richtig eingesetzt, in einem Forschungsdesign weniger einschränken als befähigen.

Die politische Landschaft

Dieser Abschnitt wurde von Armida van Rij und Lucy Thomas, beide Research Associates am Policy Institute des King's College London, verfasst. Er bietet einen Überblick über den politischen Kontext des Berichtsthemas.

Einleitung

Die Erforschung terroristischer und/oder extremistischer Inhalte wirft seit Jahrzehnten für Forschende, Regierungen, Aktivisten und Strafverfolgungsbehörden gleichermaßen anspruchsvolle Fragen zur Legalität, Moral und Praktikabilität auf. Auf der einen Seite gibt es die Datenschutzgesetze und die Einschränkungen, an die sich Forschende beim Umgang mit personenbezogenen Daten halten müssen. Auf der anderen Seite gibt es die Gesetzgebung rund um die Terrorismusbekämpfung und die Art und Weise, wie Daten von Terroristen und Extremisten für Forschungszwecke verwendet werden dürfen. Hieraus ergibt sich ein zunehmend komplexes Feld, in dem sich Forschende bewegen müssen, mit Risiken für sich selbst und andere.

In diesem Bericht werden wir einen etwas anderen Ansatz als in früheren Berichten verfolgen, indem wir zunächst die politische Landschaft zum Schutz von personenbezogenen Daten in acht der neun Länder behandeln. Anschließend gibt der Bericht einen detaillierten Überblick über die Landschaft der Terrorismusbekämpfung im neunten Land, dem Vereinigten Königreich, und geht auf einige der schwierigen Fragen ein, auf die Forschende, die sich für Terrorismusforschung interessieren, stoßen können.

Datenschutz auf Social-Media-Plattformen: Umgang mit den Herausforderungen und Beurteilung neuer Entwicklungen

Kanada

Für den Schutz und die Förderung der Datenschutzrechte des Einzelnen ist das Office of the Privacy Commissioner of Canada (OPC) zuständig. Das Mandat des OPC umfasst die Durchsetzung der Einhaltung sowohl des Privacy Act, der regelt, wie die Bundesbehörden mit personenbezogene Daten umgehen, als auch des Personal Information Protection and Electronic Documents Act (PIPEDA), der für den privaten Sektor gilt. PIPEDA ist ein Bundesgesetz, aber die Provinzen Alberta, British Columbia und Québec haben eigene Datenschutzgesetze, die sich im Wesentlichen ähneln.[53]

53 ‚PIPEDA in brief', Office of the Privacy Commissioner of Canada. Abgerufen: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_brief/

Generell verpflichtet PIPEDA private Organisationen dazu, „die Zustimmung einer betroffenen Person einzuholen, wenn sie personenbezogene Daten dieser Person erfassen, verwenden oder weitergeben," und die gesetzlichen Vorschriften zum Schutz dieser Daten einzuhalten. Gemäß PIPEDA müssen Unternehmen zehn „Grundsätze der fairen Information" einhalten, um den Schutz der Rechte der Einzelperson an ihren Daten zu gewährleisten, darunter Rechenschaftspflicht, Einwilligung, Begrenzung der Erfassung, Begrenzung der Verwendung, Offenlegung und Aufbewahrung, Korrektheit und Schutzmaßnahmen.[54]

Neben „Horizon Scanning" zur Erforschung neuer Technologien und ihrer Auswirkungen auf die Datenrechte der kanadischen Bevölkerung verleiht[55] PIPEDA dem OPC auch Befugnisse zur Rechtsdurchsetzung bei Datenschutzverletzungen. Zu diesen Durchsetzungsbefugnissen gehören Ermittlungsbefugnisse und Geldstrafen –Unternehmen, die Datenschutzverletzungen nicht an das OPC melden, können mit einer Geldstrafe von bis zu 100.000 C$ belegt werden. Ähnlich wie in Neuseeland liegt dieses Bußgeld weit unter den Geldstrafen anderer Rechtssysteme, wie zum Beispiel den 20.000.000 € der EU-DSGVO (bzw. bis zu 4 % des Jahresumsatzes).

Im November 2020 hat Kanadas Minister of Innovation, Science and Industry ein neues Gesetz zum Schutz personenbezogener Daten vorgelegt. In einer Pressemitteilung führte das Ministerium die Coronavirus-Pandemie als Kontext für die Modernisierung und Aktualisierung der Datenschutzgesetze an, da viel mehr Menschen Technologie nutzen, um miteinander zu kommunizieren.[56]

Das neue Gesetz, der Digital Charter Implementation Act (DCIA), würde ein neues Datenschutzgesetz für den privaten Sektor einschließlich der Social-Media-Plattformen implementieren. Der DCIA sieht weitaus stärkere Aufsichts- und Durchsetzungsbefugnisse für Verstöße vor – bis zu 5 % des Umsatzes oder 25 Millionen C$ – und verlangt von den Unternehmen Transparenz in Bezug auf ihre Nutzung von Algorithmen und künstlicher Intelligenz. Gemäß DCIA müssten „Unternehmen transparent machen, wie sie solche Systeme nutzen, um zu relevanten Vorhersagen, Empfehlungen oder Entscheidungen für Einzelpersonen zu kommen. Einzelpersonen könnten zudem von Unternehmen verlangen, dass diese erklären, wie eine Vorhersage, Empfehlung oder Entscheidung durch ein automatisiertes Entscheidungssystem zustande gekommen ist und wie sie an die Informationen gekommen sind."[57] In Ghana enthält das Datenschutzgesetz von 2012 eine ähnliche Klausel (siehe unten).

54 Ebd.
55 ‚Research', Office of the Privacy Commissioner of Canada. Abgerufen: https://www.priv.gc.ca/en/opc-actions-and-decisions/research/
56 ‚New proposed law to better protect Canadians' privacy and increase their control over their data and personal information', kanadische Regierung, 17. November 2020. Abgerufen: https://www.canada.ca/en/innovation-science-economic-development/news/2020/11/new-proposed-law-to-better-protect-canadians-privacy-and-increase-their-control-over-their-data-and-personal-information.html
57 ‚Fact Sheet: Digital Charter Implementation Act, 2020', kanadische Regierung. Abgerufen: https://www.ic.gc.ca/eic/site/062.nsf/eng/00119.html

Europäische Kommission

Im Rahmen der Initiative der Europäischen Kommission, „Ein Europa für das digitale Zeitalter" hat sich die EK der Regulierung der zahlreichen Facetten digitaler Dienste angenommen. Hierzu zählen auch der Schutz personenbezogener Daten und der Privatsphäre. Der Datenschutz in der Europäischen Union wird durch die Datenschutzgrundverordnung (DSGVO) geregelt, die 2016 in Kraft getreten ist. Sie soll „das Grundrecht der Bürger und Bürgerinnen auf Datenschutz schützen, wenn personenbezogene Daten von Strafverfolgungsbehörden für Strafverfolgungszwecke verwendet werden" und „stellt vor allem sicher, dass die Daten von Opfern, Zeugen und Verdächtigen bei strafrechtlichen Ermittlungen ausreichend geschützt sind, und erleichtert die grenzübergreifende Zusammenarbeit im Kampf gegen Kriminalität und Terrorismus".[58] Entscheidend dabei ist, dass sie für alle Unternehmen gilt, die auf dem europäischen Markt tätig sind, unabhängig davon, wo sie ihren Sitz haben. Das bedeutet, dass auch Unternehmen wie Google sich an die DSGVO-Grundsätze halten müssen. Anderenfalls riskieren sie, mit einem Bußgeld belegt und/oder verklagt zu werden.

Mit der DSGVO wurde das Amt des Europäischen Datenschutz-beauftragten implementiert. Dabei handelt es sich um eine unabhängige EU-Einrichtung, deren Aufgabe die Überwachung der Anwendung der Datenschutzvorschriften und die Untersuchung von Beschwerden umfasst.[59]

Die DSGVO schützt nicht nur die Rechte der Bürgerinnen und Bürger, sondern gibt den zuständigen Behörden auch die Instrumente an die Hand, um die Einhaltung der Vorschriften zu gewährleisten und zielt darauf ab, die Rechenschaftspflicht derjenigen zu erhöhen, die personenbezogene Daten verarbeiten. Seit 2018, dem Zeitpunkt, zu dem alle EU-Mitgliedstaaten die DSGVO umgesetzt haben mussten, wurden Tausende von Beschwerden eingereicht und Hunderte von Geldstrafen wegen Verstößen gegen die Verordnung verhängt. Zu den spektakulärsten Fällen zählt sicherlich Frankreichs Verhängung einer Geldbuße in Höhe von 50.000.000 € gegen Google wegen „mangelnder Transparenz, unzureichender Information und fehlender gültiger Einwilligung in Bezug auf die Personalisierung von Werbeanzeigen".[60]

Neben der DSGVO existiert die Richtlinie zum Datenschutz bei der Strafverfolgung. Die Richtlinie 2016/680 bezieht sich auf die Verarbeitung personenbezogener Daten mutmaßlicher Täter, Zeugen oder Opfer von Straftaten durch die Strafverfolgungsbehörden.[61] Allerdings ist die Abgrenzung der Anwendungsbereiche der DSGVO und der Richtlinie 2016/680 unscharf, sodass die Gefahr besteht, dass ein Datenverarbeitungsvorgang in dem einen Mitgliedsstaat unter die DSGVO, in anderen aber unter die Richtlinie fällt.[62]

58 https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_de
59 Siehe https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_de
60 Siehe https://www.bbc.co.uk/news/technology-46944696
61 Siehe https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_de
62 Siehe https://www.tandfonline.com/doi/pdf/10.1080/13600869.2017.1370224?needAccess=true, p.253

Zu guter Letzt gibt es noch die EU-Richtlinie für Netz- und Informationssysteme (NIS-Richtlinie), die gesetzliche Maßnahmen zur Erhöhung der Cybersicherheit vorsieht.[63] Hierbei geht es insbesondere darum, dass die Mitgliedstaaten entsprechend gerüstet sind, die Kooperation auf EU-Ebene zu verbessern und die notwendige Infrastruktur in der gesamten EU zu stärken.[64]

Obwohl die Regulierung des Datenschutzes gewisse juristische Grenzen hat, versucht die EG auch, die ePrivacy-Verordnung (die die Datenschutzrichtlinie für elektronische Kommunikation (ePrivacy-Richtlinie) ersetzen soll) umzusetzen.[65] Diese Verordnung soll wiederum die Privatsphäre der Bürgerinnen und Bürger auf Online-Plattformen wie Messenger-Diensten schützen. Während das Europäische Parlament die ePrivacy-Verordnung (Verordnung über Privatsphäre und elektronische Kommunikation) verabschiedet hat, sind die Diskussionen auf der Ebene des Europäischen Rates ins Stocken geraten.[66] Zum Teil wurde argumentiert, dass diese Betonung des Datenschutzes im Widerspruch zu den Antiterrorgesetzen der EU stünde.[67]

Frankreich

Frankreich hat als Mitgliedstaat der EU im Mai 2018 die DSGVO und 2019 die NIS-Richtlinie umgesetzt. Sofern und sobald der Europäische Rat die Verhandlungen über die ePrivacy-Verordnung abschließen kann, wird, wie oben dargelegt, die Verordnung neben der DSGVO und der NIS-Richtlinie den Datenschutz der Bürger und Bürgerinnen regeln.

Die NIS-Richtlinie verlangt die Einrichtung einer Datenschutzbehörde. In Frankreich ist dies die Commission Nationale de l'Informatique et des Libertés (CNIL). Die CNIL hat gegen Google und andere bereits Geldbußen für Verstöße gegen die DSGVO verhängt.

Ghana

Das zentrale Werk der ghanaischen Datenschutzgesetzgebung ist der 2012 verabschiedete Data Protection Act. Ähnlich wie in Kanada und Neuseeland verlangt das Gesetz die Einrichtung einer Datenschutzkommission (Data Protection Commission, DPC), die mit Aufsichts- und Durchsetzungsbefugnissen ausgestattet ist, um die Einhaltung der gesetzlichen Vorschriften sicherzustellen.[68]

Der Data Protection Act von 2012 gilt für Datenververarbeiter bzw. -verantwortliche sowohl im öffentlichen als auch im privaten Sektor und verpflichtet sie zur Einhaltung von acht Datenschutzgrundsätzen,

63 Siehe https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive
64 Ebd.
65 Siehe https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2020:0568:FIN:EN:PDF
66 Siehe https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-jd-e-privacy-reform
67 Siehe https://www.coe.int/en/web/commissioner/-/human-rights-in-europe-should-not-buckle-under-mass-surveillance
68 Siehe https://www.dataprotection.org.gh/

unter anderem Rechenschaftspflicht, Angabe des Zwecks und Offenheit.[69] Wie in anderen Ländern hat die DPC die Befugnis, Geldstrafen gegen Datenverarbeiter bzw- verantwortliche zu verhängen, die gegen die gesetzlichen Vorschriften verstoßen.

Einer der innovativsten Aspekte des ghanaischen Datenschutzgesetzes – vor allem wenn man bedenkt, dass es bereits 2012 verabschiedet wurde – ist eine Klausel, die der Einzelperson das Recht auf Freiheit von automatisierten Entscheidungen einräumt. Diese Klausel besagt, dass „wichtige Entscheidungen über Ihre Person, die auf Ihren personenbezogenen Daten beruhen, von einem Menschen getroffen werden müssen und nicht automatisch generiert werden dürfen, es sei denn, Sie stimmen dem zu".[70] Dieses moderne und einwilligungsbasierte Modell für die automatisierte und algorithmische Datenverarbeitung hat potenziell weitreichende Folgen für die Art und Weise, wie Forschende auf Social-Media-Daten zugreifen und diese mithilfe von Software verarbeiten können. Derzeit bezieht sich die Klausel auf Informationen, die „die betreffende Person erheblich beeinträchtigen".[71] Sollte die ghanaische Regierung diese Klausel jedoch verschärfen, würde die Verwendung automatisierter Data-Scraping-Software für die Forschung schwierig.

Allerdings untergräbt der Data Protection Act 2012 derzeit die Datenrechte der Bürgerinnen und Bürger durch eine Klausel, wonach „personenbezogene Daten, die zu Forschungszwecken verarbeitet werden ... auf unbestimmte Zeit aufbewahrt werden dürfen".[72] Außerdem gilt: „Personenbezogene Daten, die nur zu Forschungszwecken verarbeitet werden, sind von den Bestimmungen dieses Gesetzes ausgenommen, wenn die Daten unter Einhaltung der entsprechenden Bedingungen verarbeitet werden".[73] Dies schmälert die Datenrechte von Einzelpersonen ganz erheblich, weil Forschende die Mindestanforderungen des Datenschutzes erfüllen und die Daten ansonsten auf unethische Weise verarbeiten können. Die weit gefasste und vage Definition von „Forschung" bedeutet zudem, dass die Rechte der Einzelperson an ihren Daten relativ leicht gefährdet werden können.

Japan

Die Bestimmungen zum Datenschutz sind in Japan durch den Act on the Protection of Personal Information 2003 (APPI) festgelegt. Die Zuständigkeit für die Durchsetzung der Bestimmungen des APPI liegt bei der Personal Information Protection Commission (PPC). Die Datenschutzaufsichtsbehörde wurde 2016 gegründet, um die zuvor uneinheitlichen Aufgaben der Regulierungsbehörden zu zentralisieren.

69 ‚The Data Protection Principles', Data Protection Commission. Abgerufen: https://www.dataprotection.org.gh/data-protection/data-protection-principles
70 ‚Data Protection for Individuals', Data Protection Commission. Abgerufen: https://www.dataprotection.org.gh/data-protection/data-protection-for-individuals
71 Data Protection Act 2012, Para. 41. Abgerufen: https://www.dataprotection.org.gh/index.php/resources/downloads/data-protection-act/38-data-protection-act-2012-act-843
72 Ebd., § 65.
73 Ebd.

Die PPC hat vergleichsweise geringe Aufsichts- und Durchsetzungsbefugnisse: Datenschutzverstöße können zwar Geld- und Haftstrafen nach sich ziehen, doch sind die Bußgelder mit bis zu 300.000 ¥ (knapp 2.400 €) extrem niedrig.[74] Der APPI besteht auch nicht auf direkten Verpflichtungen für Stellen, die personenbezogene Daten verarbeiten, sondern schreibt eher lockere Aufsichts- und Anleitungsmaßnahmen vor. Dies ist besonders wichtig für die akademische Forschung, da der APPI in seinem territorialen Geltungsbereich über Japan hinausgeht. So verpflichtet der Umgang mit personenbezogenen Daten japanischer Staatsangehöriger lediglich zur Einhaltung dieser lockeren Vorschriften – auch wenn dieser Umgang außerhalb Japans stattfindet.

Der APPI wurde 2020 umfassend überarbeitet und geändert. Im Gegensatz zum allgemeinen weltweiten Trend zur Stärkung der Betroffenenrechte werden die Pflichten von Datenverarbeitern durch die Änderungen von 2020 deutlich gelockert. Bei pseudonym verarbeiteten Informationen kann der Zweck der Datennutzung über den Umfang des ursprünglichen Verwendungszwecks hinaus geändert werden und die Pflichten zur Benachrichtigung der PPC über Datenschutzverstöße können entfallen. Außerdem haben Einzelpersonen nicht mehr das Recht, ihre Daten abzurufen, zu korrigieren oder die Einstellung der Nutzung zu verlangen.[75]

Ein weiterer Rückschlag für die Rechte der Datensubjekte ist der Umstand, dass Forschende vom APPI ausgenommen sind, da dieser „nur für Personen oder Einrichtungen gilt, die personenbezogene Daten im Rahmen ihrer Geschäftstätigkeit verarbeiten".[76] Konkret bedeutet dies, dass japanische Bürgerinnen und Bürger, deren personenbezogene Daten von Forschenden eingesehen und verarbeitet werden, nur sehr wenige Datenschutzrechte haben.

Neuseeland

In Neuseeland obliegt der Schutz personenbezogener Informationen und Daten dem Office of the Privacy Commissioner (OPC). Die Datenschutzbehörde wurde 1993 im Rahmen des im selben Jahr verabschiedeten Privacy Act, dem ersten substantiellen Gesetz Neuseelands zur Regelung des Umgangs mit personenbezogenen Daten, gegründet Dieses Gesetz regelt, wie personenbezogene Daten „erfasst, verwendet, offengelegt, gespeichert und zugänglich gemacht werden dürfen".[77] Die Funktionen des OPC sind dabei sowohl reaktiv als auch proaktiv: Die Datenschutzbehörde prüft nicht nur Beschwerden zu Verstößen gegen den Schutz der Privatsphäre und setzt die Einhaltung des Privacy Act durch, sondern beobachtet auch die Entwicklungen neuer Technologien unter dem Aspekt möglicher Auswirkungen auf den Schutz personenbezogener Daten.[78]

74 Act on the Protection of Personal Information 2003, § 56. Abgerufen: https://www.cas.go.jp/jp/seisaku/hourei/data/APPI.pdf
75 ‚Japan – Data Protection Overview', Data Guidance. Abgerufen: https://www.dataguidance.com/notes/japan-data-protection-overview
76 Ebd.
77 ‚What is personal information and the Privacy Act?', Data.govt.nz. Abgerufen: https://www.data.govt.nz/manage-data/privacy-and-security/what-is-personal-identifiable-information-and-the-privacy-act/
78 ‚What we do', Office of the Privacy Commissioner. Abgerufen: https://www.privacy.org.nz/about-us/what-we-do/

Im Dezember 2020 trat in Neuseeland eine neue Gesetzgebung zum Schutz personenbezogener Daten in Kraft: der Privacy Act 2020. Das neue Gesetz wurde „als Antwort auf die Art und Weise" eingebracht, „wie die Technologie den Umgang mit personenbezogenen Daten revolutioniert hat",[79] nachdem sich die Art und der Umfang der personenbezogenen Daten seit 1993 fast bis zur Unkenntlichkeit verändert haben. Vor diesem Hintergrund sind die Änderungen am Gesetz von 1993 bemerkenswert gering; Der derzeitige Datenschutzbeauftragte begründete dies damit, dass „der Privacy Act ein technologieneutrales Gesetzeswerk mit einem prinzipienbasierten Ansatz" sei, „der es gegenüber technologischen Veränderungen widerstandsfähig gemacht" habe.[80]

Die wichtigste Änderung im neuen Gesetz ist der Schutz der personenbezogenen Daten von Personen mit neuseeländischer Staatsbürgerschaft im Ausland: Informationen dürfen nun nicht mehr „ins Ausland weitergegeben werden, wenn dort keine Schutzmaßnahmen greifen, die mit dem neuseeländischen Recht vergleichbar sind".[81] Der Privacy Act 2020 umfasst zudem ausdrücklich eine „extraterritoriale Anwendbarkeit", wonach jedes in Neuseeland tätige Unternehmen den Datenschutzauflagen unterliegt, auch wenn es dort keine physische Präsenz hat.[82] Diese juristischen Aspekte sind interessant, da viele große Technologie- und Social-Media-Unternehmen ihren Sitz im Ausland haben, insbesondere in den Vereinigten Staaten – wo schwächere Datenschutzgesetze gelten. Da viele Länder ähnliche Gesetze erlassen haben, steigt der internationale Druck auf die USA, ihre eigenen Datenschutzgesetze zu verschärfen, um mit den Auflagen außerhalb des eigenen Landes Schritt zu halten.

Mit dem Privacy Act 2020 erhält das OPC auch größere Durchsetzungsbefugnisse, einschließlich einer Erhöhung der maximalen Geldstrafe für Verstöße gegen die Datenschutzgrundsätze von 2.000 NZ$ auf 10.000 NZ$. Im internationalen Vergleich liegt dieses Strafmaß weit unter demjenigen anderer Regionen oder Länder, beispielsweise den bis zu 20.000.000 € (bzw. bis zu 4 % des Jahresumsatzes) der EU-DSGVO oder Australiens Maximum von 10.000.000 AU$. Außerdem hat das neue neuseeländische Gesetz kein Pendant zum „Recht auf Vergessenwerden" der DSGVO, wonach Einzelpersonen die Löschung ihrer personenbezogenen Daten verlangen können.[83] Dieses Recht ist aus datenethischer Sicht besonders relevant für die Forschung, da Nutzer, die extremistische Inhalte auf Social-Media-Plattformen posten – Inhalte, die zu Forschungszwecken verwendet werden können – das Recht haben, diese zu löschen.

79 ‚Input of the New Zealand Human Rights Commission: OHCHR Report on the Right to Privacy in the Digital Age', United Nations Human Rights Office of the High Commissioner, 10. April 2018. Abgerufen: https://www.ohchr.org/Documents/Issues/DigitalAge/ReportPrivacyinDigitalAge/HRC_NewZealand.pdf

80 ‚Media Release: Privacy Act turns 25', Office of the Privacy Commissioner, 19. Februar 2018. Abgerufen: https://www.privacy.org.nz/assets/Uploads/2018-02-19.pdf

81 ‚Privacy Act 2020: One Small Step for New Zealand, but No Giant Leaps in Sight', Equal Justice Project, 31 August 2020. Abgerufen: https://www.equaljusticeproject.co.nz/articles/37tbkho3ex74g87sw2n6yz6beyso4a2020

82 ‚Privacy 2.0: Key changes in the Privacy Act 2020', Office of the Privacy Commissioner, 16. Juni 2020. Abgerufen: https://www.privacy.org.nz/blog/key-changes-in-the-privacy-act-2020/

83 ‚Privacy Act 2020', Equal Justice Project, 31. August 2020. Abgerufen: https://www.equaljusticeproject.co.nz/articles/37tbkho3ex74g87sw2n6yz6beyso4a2020

Counter-Terrorism Committee Executive Directorate der Vereinten Nationen

Innerhalb des Systems der Vereinten Nationen fällt der Datenschutz in den Arbeitsbereich der Konferenz der Vereinten Nationen für Handel und Entwicklung (United Nations Conference on Trade and Development, UNCTAD). Die UNCTAD hat die Notwendigkeit eines ausgewogenen Verhältnisses von Datenschutz und Überwachung und die damit verbundenen Herausforderungen diskutiert. Sie hat beschrieben, wie nach einem spektakulären Gerichtsfall, der an den Europäischen Gerichtshof verwiesen wurde, nun „die Richtung für Bedingungen und Beschränkungen für die Überwachung in allen Datenschutzsystemen in Europa vorgegeben ist, was Auswirkungen auf alle Länder haben wird, die sich am europäischen Recht orientieren“.[84]

Die Rechtsprechung ist ebenfalls ein enorm schwieriger Bereich, besonders wenn es um den Online-Datenschutz geht. Die UNCTAD verweist darauf, dass die DSGVO in Artikel 3 eine Extraterritorialitätsklausel enthalte, die einen „lokalen Datenschutz“ für Bürgerinnen und Bürger der EU gewährleisten soll, unabhängig vom Sitz des Unternehmens.[85]

USA

Im Gegensatz zu vielen anderen Nationen haben die USA kein zentrales Bundesdatenschutzgesetz. Stattdessen gibt es mehrere Datenschutzgesetze, die einzelne Aspekte des Datenschutzes regeln. So werden beispielsweise Gesundheitsdaten durch den Health Insurance Portability and Accountability Act 1996 geschützt, während personenbezogene Daten im Besitz der Regierung dem US Privacy Act von 1974 unterliegen.

Wesentlich ist, dass personenbezogene Daten und der Datenschutz im Internet in den Vereinigten Staaten derzeit keiner bundesstaatlichen Regelung unterliegen. In den USA ist das Internet so etwas wie ein regulatorischer „Wilder Westen“, wo Einzelpersonen, Gruppen, Organisationen und Unternehmen ohne besondere datenrechtliche Regelungen auf Daten zugreifen und diese verarbeiten können.

Derzeit ist die einzige Möglichkeit zum Schutz der Rechte an personenbezogenen Daten auf Social-Media-Plattformen die Federal Trade Commission (FTC). 2019 konnte die FTC beispielsweise Facebook eine enorme Geldstrafe in Höhe von 5.000.000.000 US$ für Datenschutzverletzung im Rahmen des Cambridge Analytica-Skandals auferlegen.[86] Die FTC prüfte und bestrafte Facebook im Rahmen ihrer Befugnisse gemäß Paragraf 5, der sich auf „unlautere oder irreführende Handlungen und Praktiken“ bezieht.” Facebook hatte die personenbezogenen Daten von Nutzern an

84 Siehe https://unctad.org/system/files/official-document/dtlstict2016d1_en.pdf, S. 16
85 Ebd., S. 20.
86 Julia Carrie Wong, ‚Facebook to be fined $5bn for Cambridge Analytica privacy violations – reports‘, *The Guardian*, 12. Juli 2019. Abgerufen: https://www.theguardian.com/technology/2019/jul/12/facebook-fine-ftc-privacy-violations

Apps von Drittanbietern weitergegeben, die „Freunde“ der Nutzer heruntergeladen hatten. Da zahlreiche Nutzer keine Kenntnis von diesen Praktiken und keine Möglichkeit hatten, diese abzulehnen, handelte es sich hierbei um eine unlautere oder irreführende Handlung.[87] Dieser juristische Punkt ist wichtig, denn er bedeutet, dass ein Unternehmen, das keine Informationen über seine Datenverarbeitung oder -handhabung offenlegt, nicht aufgrund der Klausel für „unlauteren oder irreführenden Handlungen oder Praktiken“ haftbar gemacht werden kann.

Einige wenige Bundesstaaten haben Verbraucherdatenschutzgesetze verabschiedet, allen voran Kalifornien. Da viele der großen Social-Media- und Technologieunternehmen ihren Sitz in Kalifornien haben, ist die dortige Datenschutzregulierung von großer Relevanz. Der California Online Privacy Protection Act aus dem Jahr 2004 war das erste Gesetz, das Websites dazu verpflichtete, ihre Datenschutzrichtlinien zu veröffentlichen. Vor allem aber gilt dies für jede Website, auf die kalifornische Bürgerinnen und Bürger zugreifen können. Hierdurch sind praktisch alle amerikanischen Websites an die Einhaltung dieser Vorschrift gebunden.

Am 1. Januar 2020 trat der California Consumer Privacy Act (CCPA) in Kraft. Der CCPA ist ein Meilenstein für den Datenschutz in den USA, denn er gilt für „gewinnorientierte Unternehmen, die in Kalifornien Geschäfte machen“ oder andere Bedingungen hinsichtlich ihrer Einnahmen und der Daten von in Kalifornien wohnhaften Personen erfüllen. In der Praxis heißt das, dass viele große Technologie- und Social-Media-Unternehmen in den Anwendungsbereich des CCPA fallen. Der CCPA gibt Einzelpersonen das Recht zu wissen, welche personenbezogenen Daten über sie erfasst werden, das Recht auf Löschung dieser Daten und das Recht, dem Verkauf ihrer personenbezogenen Daten zu widersprechen. Unternehmen sind verpflichtet, Verbraucher über ihre Datenschutzpraktiken zu informieren.[88]

Die Verabschiedung des CCPA und die Bestrafung von Facebook durch die FTC signalisieren einen politischen Willen in den USA, die Datenrechte von Einzelpersonen zu schützen. Im Februar 2020 schlug Senatorin Kirsten Gillibrand ein weitreichendes Datenschutzgesetz vor, das eine unabhängige Bundesbehörde zur Durchsetzung der Datenschutzbestimmungen einrichten sollte.[89] Obwohl das nicht ausreicht, um spezielle Datenschutzrechte und -pflichten für alle amerikanischen Staatsangehörigen zu gewährleisten, deutet es darauf hin, dass sich die USA möglicherweise in Richtung einer Bundesgesetzgebung bewegen.

87 ‚FTC Imposes $5 Billion and Sweeping New Privacy Restrictions on Facebook‘, Federal Trade Commission, 24. Juli 2019. Abgerufen: https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions

88 ‚California Consumer Privacy Act‘, State of California Department of Justice. Abgerufen: https://oag.ca.gov/privacy/ccpa

89 ‚A run-down of US Sen. Gillibrand's proposed Data Protection Act‘, International Association of Privacy Professionals, 21. Februar 2020. Abgerufen: https://iapp.org/news/a/an-run-down-of-sen-gillibrands-proposed-data-protection-act/

Erforschung extremistischer Inhalte in Großbritannien: Prevent, Gesetzgebung zur Terrorismusbekämpfung und politische Entwicklungen

Nach den Terroranschlägen vom 11. September 2001 in New York und auf das Pentagon in den USA verschärften viele westliche Nationen ihre internen Sicherheitsmaßnahmen, um Anschläge auf eigenem Boden zu verhindern. Die Anti-Terror-Politik im Westen beschäftigte sich zunehmend mit dem Begriff der Radikalisierung – dem Phänomen, dass Einzelpersonen sich sukzessive mit terroristischen Werten identifizieren, diese schließlich unterstützen oder sogar gewalttätige Angriffe zu terroristische Zwecken ausführen können. Dieser Prozess der Radikalisierung wird auf eine Vielzahl von sozialen und individuellen Faktoren zurückgeführt: Kontakt mit Ideologien, Viktimisierung, Entfremdung, Sozialisation, soziale Netzwerke, das Internet, Defizite in den familiären Bindungen, Traumata, relative soziale und wirtschaftliche Benachteiligung sowie „Kulturen der Gewalt".[90] Angesichts der Vielzahl möglicher ‚Radikalisierungswege' sind die Regierungen zu der Überzeugung gelangt, dass sie künftige Terroranschläge durch eine Reihe von Eingriffen ins Alltagsleben verhindern können".[91]

2003 startete das britische Home Office (Innenministerium) die Prevent-Strategie als Teil seiner umfassenderen Strategie zur Terrorismusbekämpfung, CONTEST. Prevent wurde 2011 überarbeitet und neu aufgelegt, um Personen zu erreichen, die „anfällig" für Radikalisierung sind,[92] insbesondere innerhalb von zivilen Institutionen wie Schulen, registrierten Kinderbetreuungseinrichtungen, Universitäten, Hochschulen, Gefängnissen, Bewährungshilfe, Gesundheitswesen, Sozialdiensten und Einwanderungsbehörden. Die Prevent-Strategie gilt dem „prä-kriminellen Raum"[93] – sie greift ein, bevor irgendeine kriminelle Aktivität stattgefunden hat, in der Hoffnung, den Prozess der Radikalisierung aufzuhalten.[94]

Prevent zielt darauf ab, „Personen zu unterstützen und vom falschen Weg abzubringen, die gefährdet sind oder dabei sind, für terroristische Aktivitäten präpariert/radikalisiert zu werden, bevor ein Verbrechen begangen wird".[95] Durch Formulierung von Prevent als eine vorbeugende und nicht als eine kriminalisierende Maßnahme wird das Programm eher als schützend denn als repressiv positioniert. Aus dieser Darstellungsweise ergibt sich, dass die Verantwortung für die Durchführung von Prevent zivilgesellschaftlichen Institutionen zufällt. Diese Institutionen, beispielsweise Hochschulen, sind im Rahmen ihrer Fürsorgepflicht verpflichtet, mögliche Fälle von Radikalisierung vorherzusehen, zu beobachten und zu intervenieren. Es bedeutet auch, dass Arbeitgeber und Beschäftigte auf eine unmöglich große,

90 Katherine E. Brown & Tania Saeed (2015), ‚Radicalization and counter-radicalization at British universities: Muslim encounters and alternatives', *Ethnic and Racial Studies*, Bd. 38 Nr. 11, S. 1952–68.
91 Ebd.
92 ‚Prevent Strategy' Britische Regierung, Juni 2011. Abgerufen: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/97976/prevent-strategy-review.pdf
93 David Goldberg, Sushrut Jadhav und Tarek Younis (2017), ‚Prevent: What is Pre-Criminal Space?', *British Journal of Psychology* Bulletin, Bd. 41 Nr. 4, S. 208–11.
94 Interessanterweise wurde der Begriff „pre-crime" („Prä-Verbrechen") von Philip K. Dick, dem Autor der Science-Fiction-Kurzgeschichte *Minority Report* (Der Minderheitenbericht) geprägt. Siehe: Goldberg, Jadhav und Younis, S. 208–11.
95 Charlotte Heath-Kelly und Erzsébet Strausz, ‚Counter-terrorism in the NHS: Evaluating Prevent Duty Safeguarding in the NHS', University of Warwick. Abgerufen: https://warwick.ac.uk/fac/soc/pais/research/researchcentres/irs/counterterrorisminthenhs/project_report_60pp.pdf

komplexe und vage definierte Anzahl von Indikatoren achten müssen, die darauf hindeuten, dass eine Person anfällig für Radikalisierung ist. In diesem Umfeld gehen die Institutionen verständlicherweise übervorsichtig vor.

In den ersten Jahren konzentrierte sich die Prevent-Strategie an den Hochschulen auf studentische Communitys, insbesondere auf britische muslimische Studierende. So begannen die Einrichtungen, Vorlesungen, Vortragsveranstaltungen und Veranstaltungen der Studentenvereinigungen zu kontrollieren, um die Prevent-Strategie einzuhalten und jegliche Zweifel daran auszuräumen, dass innerhalb der Hochschule keine extremistischen Überzeugungen verherrlicht werden. Es gibt zahllose Beispiele dafür, dass muslimische Studierende im Rahmen von Prevent auf dem Campus unverhältnismäßig ins Visier genommen und befragt wurden,[96] darunter ein Student, der an das Sicherheitsteam der Universität Staffordshire überstellt wurde, weil er im Rahmen seines Aufbaustudiums ein Fachbuch über Terrorismus, Kriminalität und globale Sicherheit gelesen hatte.[97] Fast 2.500 Veranstaltungen an rund 300 Hochschulen wurden 2017–18 entweder abgesagt oder geändert (indem zum Beispiel Referenten ausgeladen wurden).

Das Bild ist besonders komplex, wenn es um akademisch Forschende geht, die Extremismus und Terrorismus untersuchen. Der Kontakt mit extremistischen und terroristischen Inhalten und Werten ist durchaus offensichtlich und direkt, da die Forschung oft den Zugang zu und die Sammlung von terroristischen und extremistischen Inhalten voraussetzt, wie offizielle Erklärungen terroristischer Gruppen, terroristische Propaganda (einschließlich visueller Medien), pro-extremistische Beiträge in sozialen Medien, Messageboards im Internet usw. Insbesondere Methoden der Feldforschung, wie Interviews mit verurteilten Terroristen oder radikalisierten Personen, bedeuten für Forschende ständigen Kontakt mit Personen, die als extremistisch oder terroristisch eingestuft sind.

Hieraus ergeben sich interessante Fragen zu Risiken der Forschung: können und müssen akademisch Forschende als anfällig für Radikalisierung angesehen werden? Welche Konsequenzen ergeben sich daraus aus rechtlicher und politischer Sicht? Welche Auswirkungen hat dies auf die Forschung und Forschenden?

Was die Extremismusforschung angeht, sind die wichtigsten Gesetze zur Terrorismusbekämpfung in Großbritannien der Terrorism Act von 2000 und der Terrorism Act 2006. Paragraf 57 und 58 des Gesetzes von 2000 stellten den Besitz von Materialien unter Strafe, die „Anlass zu dem begründeten Verdacht geben, dass ihr Besitz einem Zweck dient, der mit der Begehung, Vorbereitung oder Anstiftung einer terroristischen Handlung verbunden ist“[98] oder von Informationen,

96 ‚The Impact of Prevent on Muslim Communities: A Briefing to the Labour Party on how British Muslim Communities are Affected by Counter-Extremism Policies‘, The Muslim Council of Britain, Februar 2016. Abgerufen: http://archive.mcb.org.uk/wp-content/uploads/2016/12/MCB-CT-Briefing2.pdf; Barbara Cohen und Waqas Tufail, ‚Prevent and the normalization of Islamophobia‘, *Islamophobia: Still a challenge for us all*, Runnymede Trust. Abgerufen: https://core.ac.uk/download/pdf/161895664.pdf

97 Randeep Ramesh und Josh Halliday, ‚Student accused of being a terrorist for reading book on terrorism‘, *The Guardian*, 24. September 2015. Abgerufen: http://www.theguardian.com/education/2015/sep/24/student-accused-being-terrorist-reading-book-terrorism

98 *Terrorism Act 2000*, § 57. Abgerufen: https://www.legislation.gov.uk/ukpga/2000/11/section/57

die „wahrscheinlich für eine Person, die eine terroristische Handlung begeht oder vorbereitet, nützlich sind".[99] Mit anderen Worten ist jedweder Besitz von Informationen oder Material in Zusammenhang mit Extremismus oder Terrorismus eine Straftat, insbesondere wenn diese Informationen Einzelpersonen oder Gruppen dabei helfen könnten, andere zu rekrutieren oder zu radikalisieren oder gewalttätige Angriffe zu verüben.

Das Anti-Terror-Gesetz von 2006 baut auf den Straftatbeständen des Material- und Informationsbesitzes des Gesetzes von 2000 auf und erweitert diese. Es erfasst nun auch die Verbreitung dieser Materialien (Paragraf 1) und schafft einen Straftatbestand für die Verherrlichung von Terrorismus (unter anderem auch durch den Besitz und die Verbreitung dieser Materialien, Paragraf 2). Der erste Paragraf bezieht sich auf Einzelpersonen oder Gruppen, die beabsichtigen, „direkt oder indirekt [andere] zu ermutigen oder anderweitig zu veranlassen, terroristische Handlungen zu begehen, vorzubereiten oder anzustiften",[100] einschließlich Aussagen, die „die Begehung oder Vorbereitung ... solcher Handlungen verherrlichen".[101] Darüber hinaus gilt dieser Straftatbestand für alle britischen Staatsbürger und Staatsbürgerinnen, einschließlich Forschende, auch wenn sie sich im Ausland aufhalten.[102] Demnach könnte sich eine forschende Person mit einem Stipendium im Ausland aufhalten oder Feldforschung betreiben und trotzdem nach britischem Recht wegen Förderung des Terrorismus angeklagt werden. Der zweite Paragraf betrifft die Verbreitung von terroristischen Publikationen. Konkret kriminalisiert er die Verteilung, die Verbreitung, das Verschenken, den Verkauf, das Verleihen, das Anbieten und den elektronischen Versand von terroristischen Publikationen oder die Erbringung von Dienstleistungen für andere, die es ermöglichen, diese Publikationen zu erhalten, zu lesen, zu hören, anzusehen, zu erwerben, zu kaufen oder zu leihen.[103]

Die Probleme, die sich dadurch für die Wissenschaft ergeben, die sich in Lehre und Forschung mit Extremismus und Terrorismus auseinandersetzt, liegen auf der Hand. Ein Dozent, der beispielsweise in seinem Seminar ein Propagandavideo des so genannten Islamischen Staates zeigt, könnte sich gleich mehrerer Straftaten schuldig machen: des Besitzes von terroristischem Material, der indirekten Ermutigung anderer zur Begehung terroristischer Handlungen und der Verbreitung terroristischer Publikationen.

Der als „Nottingham Two" bekannt gewordene Fall ist ein konkretes Beispiel. Im Mai 2008 schrieb Rizwaan Sabir, Masterstudent an der Universität von Nottingham, eine E-Mail an seinen akademischen Berater, Hicham Yezza, um seinen Forschungsvorschlag für die Promotion über islamischen Terrorismus vorzubereiten. Sabir hatte die Website des US-Justizministeriums durchsucht und ein Regierungsdokument mit dem Titel „Military Studies in the Jihad Against the Tyrants: the Al-Qaeda Training Manual" (das in einem Gerichtsverfahren zur Strafverfolgung einer für Bombenanschläge in Ostafrika verantwortlichen Gruppe verwendet worden war)

99 Ebd., § 58.
100 *Terrorism Act 2006*, § 1.2 (b)(i). Abgerufen: https://www.legislation.gov.uk/ukpga/2006/11/section/1
101 Ebd., § 1.3 (a).
102 Ebd., § 17.
103 Ebd., § 2.

heruntergeladen:[104] Das Dokument war über das Bibliothekssystem der Universität frei verfügbar und kann auch in britischen Buchhandlungen wie den Läden der Waterstones-Kette erworben werden.[105] Ein Kollege bemerkte das Dokument auf Yezzas Computer und meldete es der Universität, die daraufhin die Polizei verständigte. Sowohl Sabir als auch Yezza wurden ohne Haftbefehl auf der Basis des Terrorism Act 2000 verhaftet. Sabir wurde sieben Tage lang in Isolationshaft gehalten.[106]

Das Gesetz aus dem Jahr 2000 wurde im Laufe der Zeit und in Reaktion auf verschiedene politische und gesellschaftliche Veränderungen modifiziert. Die erste wichtige Weiterentwicklung war 2015 die Verabschiedung des Counter-Terrorism and Security Act, der die Verpflichtungen der Institutionen zur Erfüllung der Prevent-Strategie forcierte. Universitäten sind nun gesetzlich verpflichtet, „der Notwendigkeit Rechnung zu tragen, dass Menschen nicht in den Terrorismus hineingezogen werden können“[107] und müssen klare Richtlinien und Verfahren für Forschende haben, die in diesem Bereich arbeiten. Das Gesetz von 2015 verlangt eine risikobasierte Herangehensweise. Das bedeutet, dass die Institutionen Forschungsaktivitäten kontinuierlich überwachen, bewerten und Maßnahmen ergreifen müssen, um die damit verbundenen Risiken zu mindern. In der Praxis haben viele Universitäten diese Prevent-Risikobewertung inzwischen in ihre forschungsethischen Abläufe integriert.[108] Die praktische Erfahrung mit diesen Abläufen legt nahe, dass die Ethikkontrollausschüsse die Risikowahrnehmung in einer Weise erweitert haben, die die institutionelle Reputation in den Vordergrund der Abwägungen stellt. Die Prevent-Strategie kann als Ermächtigung institutioneller Kontrollausschüsse gesehen werden, Anträge auf forschungsethische Prüfung – für alle Arten von „risikobehafteter, ‚politisch sensibler‘ Forschung“[109] – in komplexer und langsamer Bürokratie versinken zu lassen, in der Hoffnung, „potenzielle Gefährdungen des guten Rufs der Institution zu erschweren und im Keim zu ersticken“.[110] Dies hat im Gegenzug zu ernsthaften Bedenken im Hinblick auf die akademische Freiheit geführt.

Eine zweite große Veränderung trat im April 2019 mit der Verabschiedung des Counter-Terrorism and Border Security Act in Kraft. Mit diesem Gesetz wurden die möglichen strafrechtlichen Konsequenzen für alle oben genannten Verstöße gegen die Anti-Terror-Gesetze von 2000 und 2006 verschärft. Beispielsweise wurde die Höchststrafe für die Verbreitung terroristischer Publikationen mehr als verdoppelt, von sieben auf 15 Jahre Haft.[111]

104 Rizwaan Sabir, ‚Damages for my unjust „terror“ arrest‘, *Al Jazeera*, 21. September 2011. Abgerufen: https://www.aljazeera.com/opinions/2011/9/21/damages-for-my-unjust-terror-arrest/

105 Siehe https://www.waterstones.com/book/military-studies-in-the-jihad-against-the-tyrants/anonymous/9781907521249

106 Rizwaan Sabir und Hicham Yezza wurden ohne Anklage freigelassen. 2011 erhob Sabir Anklage gegen die Polizei von Nottinghamshire wegen unzulässiger Inhaftierung und rassistischer Diskriminierung, die außergerichtlich beigelegt wurde. Siehe Sabir, ‚Damages for my unjust „terror“ arrest‘.

107 ‚Statutory guidance: Revised Prevent duty guidance for England and Wales‘, UK Home Office, aktualisiert am 10. April 2019. Abgerufen: https://www.gov.uk/government/publications/prevent-duty-guidance/revised-prevent-duty-guidance-for-england-and-wales#c-a-risk-based-approach-to-the-prevent-duty

108 Siehe z. B. ‚Oversight of security-sensitive research material in UK universities‘, Universities UK, November 2019. Abgerufen: https://www.universitiesuk.ac.uk/policy-and-analysis/reports/Documents/2019/Oversight-security-sensitive-research-material-guidance-3.pdf

109 Adam Hedgecoe (2015), ‚Reputational Risk, Academic Freedom and Research Ethics Review‘, *Sociology*, Bd. 50 Nr. 3, S. 495.

110 Ebd.

111 *Counter-Terrorism and Border Security Act 2019*, § 7. Abgerufen: https://www.legislation.gov.uk/ukpga/2019/3/section/7

Vier neue Maßnahmen im Gesetz von 2019 sind besonders relevant für die akademische Forschung zu Extremismus und Terrorismus:

1. Das Gesetz schafft einen Straftatbestand für das Beschaffen oder Ansehen von terroristischem Material im Internet.[112]
2. Es schließt ausdrücklich Personen, die journalistische Arbeit oder akademische Forschung betreiben, vom Straftatbestand der Informationsbeschaffung (auch im Internet) aus (Paragraf 58 des Terrorism Act 2000).[113]
3. Es schafft einen Straftatbestand für Bürgerinnen und Bürger, die in ein „ausgewiesenes Gebiet" außerhalb des Vereinigten Königreichs einreisen oder sich dort aufhalten.[114] Der Secretary of State hat die Befugnis, ein solches Gebiet von Fall zu Fall zu benennen, um „Mitglieder der Öffentlichkeit vor einer Terrorgefahr zu schützen".[115]
4. Er erweitert einen Paragrafen des Terrorism Act 2006 dahingehend, dass die Verbreitung terroristischer Publikationen außerhalb des Vereinigten Königreichs als Straftat einbezogen ist (während zuvor nur die Verherrlichung von Terrorismus erfasst war).

Obiger Punkt 2 – die Ausnahme vom Verbot der Sammlung von terroristischem Material (auch im Internet) für Forschende – erscheint auf den ersten Blick als eine begrüßenswerte Entwicklung, die die akademische Freiheit wiederherstellt, zu Terrorismus und Extremismus ohne Angst vor rechtlichen Konsequenzen forschen zu können. Ein entscheidender Punkt ist jedoch, dass akademisch Forschende jetzt zwar ausdrücklich von Paragraf 58 des Terrorism Act 2000 (Besitz von terroristischem Material) ausgenommen sind, es aber keinen ausdrücklichen rechtlichen Schutz für Forschende gegen Abschnitt 1 (Verherrlichung von Terrorismus) oder 2 (Verbreitung von terroristischem Material) des Terrorism Act 2006 gibt.[116]

In der Praxis bedeutet dies, dass Forschende, die zu Forschungs- oder Lehrzwecken auf extremistisches Material im Internet zugreifen und dieses sammeln, sich wahrscheinlich auf rechtlich sicherem Grund bewegen. Würden sie Auszüge dieser Materialien jedoch in Artikeln für Zeitschriften oder Fachbüchern zitieren oder in der Lehre als Beispiele für extremistische Propaganda verwenden, ohne die Gruppen ausdrücklich zu verurteilen, könnten sich Forschende bereits in einer rechtlichen Grauzone wiederfinden. Darüber hinaus bedeutet der Terrorism Act 2000, dass Forschende ohne Haftbefehl verhaftet und bis zu 28 Tage lang festgehalten werden können, während gegen sie Anklage erhoben werden kann, wie es bei Rizwaan Sabir und Hicham Yezza geschehen ist.

Ebenso können Forschende, die Feldforschung oder Datenerfassung im Ausland betreiben, von dieser neuen Gesetzgebung betroffen sein. Forschende, die im Ausland Feldforschung in einer Region durchführen

112 Ebd., § 3.
113 Ebd., § 7.
114 *Terrorism Act 2000*, § 58(b). Abgerufen: https://www.legislation.gov.uk/ukpga/2000/11/section/58B
115 ‚Counter-Terrorism and Border Security Bill: Supplementary Delegated Powers Memorandum', UK Home Office, 5. September 2018. Abgerufen: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/739267/Supplementary-Delegated-Powers-Memo-designated-area-offence.pdf
116 „Paragraf 2 und 3 des Terrorism Act 2006 verbieten auch die Verbreitung terroristischer Publikationen, auch auf elektronischem Wege, und verwenden eine sehr weit gefasste Definition von „terroristischen Publikationen" und „Aussagen", die als Ermutigung oder Veranlassung für die Begehung, Vorbereitung oder Anstiftung zu terroristischen Handlungen ausgelegt werden können. *Akademische Forschung ist im Rahmen des Terrorism Act 2006 keine legitime Ausnahme* [Hervorhebung von mir]." ‚Oversight of security-sensitive research material in UK universities', Universities UK, November 2019. Abgerufen: https://www.universitiesuk.ac.uk/policy-and-analysis/reports/Documents/2019/Oversight-security-sensitive-research-material-guidance-3.pdf

oder planen, die der Secretary of State als „ausgewiesenes Gebiet" erklärt hat, begingen eine Straftat, wenn sie dort einreisen oder sich dort aufhalten würden.

Insgesamt ist die Rechtslage für Forschende im Bereich Terrorismus und Extremismus unklar. Obwohl die Gesetzgebung des vergangenen Jahres ein Verständnis der Regierung dafür signalisiert, dass Forschende in Besitz von kompromittierendem Material sein können, bleiben andere Gesetze unverändert, denen diese Personengruppe sehr wohl unterworfen ist. Gesetzgebung, Politik und Wissenschaft spiegeln insgesamt das derzeitige politische Klima wider und verfestigen es. In diesem Zeitalter ausgeprägter Islamophobie und breiter Unterstützung für proaktive Überwachung und Polizeiarbeit bedienen Prevent und die Anti-Terror-Gesetze sehr stark diese beiden beide Phänomene.

Ein wichtiger Faktor bei der Abwägung der Wahrscheinlichkeit, dass Forschende mit den Maßnahmen der britischen Regierung zur Terrorismusbekämpfung (wie der Prevent-Strategie) und der Gesetzgebung in Konflikt geraten, sind die unverhältnismäßigen Auswirkungen auf Muslime. Auf „islamistischen Extremismus" entfallen 65 % aller Verweise an Prevent. Das bedeutet, dass „für Muslime die Wahrscheinlichkeit, an Prevent verwiesen zu werden, im vergangenen Jahr bei ungefähr 1 zu 500 lag, d. h. etwa 40 Mal höher als bei Nichtmuslimen". In ähnlicher Weise betrafen mehr als die Hälfte (54 %) der 2017 in Großbritannien vorgenommenen terrorbezogenen Verhaftungen „nach asiatischer Herkunft aussehende" Personen.[117] Die statistische Realität ist, dass als Muslime stigmatisierte Studierende und Forschende einem weitaus größeren Risiko ausgesetzt sind, durch die rechtliche Grauzone Schaden zu erleiden – indem sie entweder an Prevent überwiesen oder sogar kriminalisiert werden.

Bislang haben wir gesehen, dass Muslime im Hochschulbereich zu Unrecht ins Visier der Anti-Terror-Gesetzgebung geraten sind. Allerdings gab es im November 2020 die bis dato höchste Anzahl von Verweisen im Zusammenhang mit Rechtsextremismus: 43 %, verglichen mit 30 % für islamistischen Extremismus.[118] Diese Entwicklung wirft interessante Fragen zum Racial Profiling und zur Forschung über Extremismus und Terrorismus auf: Werden nun nichtmuslimische Forschende als „vulnerabel" und „radikalisierungsgefährdet" betrachtet, wenn sie zum White-Supremacy-Terrorismus forschen? Und sollte das der Fall sein, welche gesellschaftlichen und politischen Reaktionen könnte dies auslösen? Eine wachsende Zahl von Kritikern versteht Prevent und die Anti-Terror-Gesetzgebung inzwischen als einen Mechanismus zur Überwachung und Kontrolle muslimischer Gemeinschaften im Hochschulbereich und darüber hinaus.[119] Wenn diese Funktion nun etabliert ist, welche Funktion kann Prevent dann noch erfüllen – wenn überhaupt eine?

117 ‚Operation of police powers under the Terrorism Act 2000 and subsequent legislation: Arrests, outcomes, and stop and search, Great Britain, financial year ending 31 March 2017', UK Home Office, Juni 2017. Abgerufen: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/619016/police-powers-terrorism-mar2017-hosb0817.pdf

118 Jamie Grierson und Dan Sabbagh, ‚Largest number of Prevent referrals related to far-right extremism', *The Guardian*, 26. November 2020. Abgerufen: https://www.theguardian.com/uk-news/2020/nov/26/just-one-in-10-prevent-referrals-found-at-risk-of-radicalisation

119 Fahid Qurashi (2018), ‚The Prevent strategy and the UK „war on terror": embedding infrastructures of surveillance in Muslim communities', *Palgrave Communications*, Bd. 4 Nr. 17 (2018); ‚Liberty's written evidence to the JCHR's Inquiry on Freedom of Expression in Universities', Liberty, Dezember 2017. Abgerufen: https://www.libertyhumanrights.org.uk/wp-content/uploads/2020/02/Libertys-Evidence-to-the-JCHRs-Inquiry-into-Freedom-of-Expression-in-Universities-Dec-2017.pdf

Schlussbemerkungen: eine sich verändernde globale Landschaft

Die ethischen und juristischen Fragen, mit denen Forschende konfrontiert sind, die auf personenbezogene Daten zugreifen und diese verarbeiten wollen, sind komplex und vielfältig. Angesichts rasanter rechtlicher und politischer Veränderungen auf nationaler und internationaler Ebene sind die globalen Aussichten für Forschende, die in den Bereichen Extremismus und Terrorismus arbeiten, von Wandel und Unsicherheit geprägt.

Was den Zugang zu Daten für Forschungszwecke angeht, gibt es generell einen globalen Trend zur Stärkung der Datenschutzgesetze, um die Datenrechte von Einzelpersonen besser zu schützen (mit einigen Ausnahmen wie Japan, siehe oben). Hieraus folgt, dass Forschende in Zukunft vermutlich stärker eingeschränkt sein werden, was die ihnen zur Verfügung stehenden Daten und die Art und Weise, wie sie diese Daten verarbeiten und nutzen können, angeht. Da die Unternehmen versuchen, mit einem Flickenteppich an nationalen und supranationalen Gesetzen Schritt zu halten, müssen Social-Media-Plattformen ihre Datenschutzrichtlinien kontinuierlich aktualisieren und ändern. Da die Konsequenzen bei Nichteinhaltung – beispielsweise die 5.000.000.000 US$ Strafe der Federal Trade Commission in den USA für Facebook – immer gravierender werden, ist es möglich, dass die Plattformen ihre Datenschutzrichtlinien konservativ gestalten, um Finanz- und Reputationssicherheit zu gewährleisten.

Die rechtlichen und politischen Rahmenbedingungen, unter denen Forschende in Zukunft im Bereich Extremismus und Terrorismus arbeiten können, sind ebenfalls unsicher. In Großbritannien hat ein Klima der proaktiven Polizeiarbeit, das mit Bedrohungen der nationalen Sicherheit begründet wird, ein politisches Umfeld geschaffen, in dem Forschende Gefahr laufen, für ihre Nähe zu bestimmten Materialien kriminalisiert zu werden. Im Zuge des „Kriegs gegen den Terror“ in den 2000er Jahren reflektierte das gesetzgeberische Umfeld in Großbritannien einen „Law-and-Order“-Ansatz zur Terrorismusbekämpfung. Dies hat zu rechtlichen Entwicklungen geführt, die das Material einschränken, auf das Forschende zugreifen, über das sie sprechen, schreiben, lehren und veröffentlichen können. Wenn sich die globale Aufmerksamkeit jedoch weg von der so genannten „islamischen Bedrohung“ und hin zu einem Bewusstsein der Existenz gewalttätiger White-Supremacy-Gruppen verschiebt, werden die bestehenden politischen und juristischen Rahmenbedingungen, die auf eine Minderheit ausgerichtet waren, problematisch.
Die gegenwärtigen Mechanismen der Denunziation im Kollegenkreis und in der Studentenschaft in den Hochschulen stützten sich zu einem großen Teil auf Racial Profiling; wie funktionieren derartige Ansätze im Hinblick auf westliche Forschende, die sich mit White-Supremacy-Themen beschäftigen?

Art und Umfang der Extremismus- und Terrorismusforschung im Westen könnten sich angesichts dieses sich verändernden globalen Kontextes in den kommenden Jahren stark verändern. So könnte es beispielsweise schwieriger werden, groß angelegte quantitative Analysen durchzuführen, wenn die Datenschutzgesetze und die Datenschutzrichtlinien von Unternehmen verschärft werden, oder auf Personen zuzugreifen, die mit terroristische Gruppen oder Taten in Verbindung stehen. In der Folge könnten sich die Methoden, die der

Extremismusforschung zur Verfügung stehen, ändern, möglicherweise stärker qualitativ ausgerichtet werden, einen kleineren Maßstab haben oder den Schwerpunkt auf digitale Ethnographie legen.[120] Obwohl diese Verschiebungen alarmierend sind, könnten auch erhebliche Vorteile erzielt werden: nähere und nuanciertere Begegnungen mit Extremismus und Terrorismus, die die Komplexität und Widersprüche von Personen mit extremistischen Überzeugungen im Internet besser reflektieren können.

120 Siehe zum Beispiel: Sarah Pink et al. (Hrsg), *Digital Ethnography: Principles and Practice* (2015), SAGE Publications Ltd.

Global Network
on Extremism & Technology

KONTAKTANGABEN

Im Falle von Fragen oder zur Anforderung weiterer Exemplare wenden Sie sich bitte an:

ICSR
King's College London
Strand
London WC2R 2LS
Vereinigtes Königreich

T. **+44 20 7848 2098**
E. **mail@gnet-research.org**

Twitter: **@GNET_research**

Wie alle anderen GNET-Publikationen kann auch dieser Bericht kostenlos von der GNET-Website unter www.gnet-research.org heruntergeladen werden.