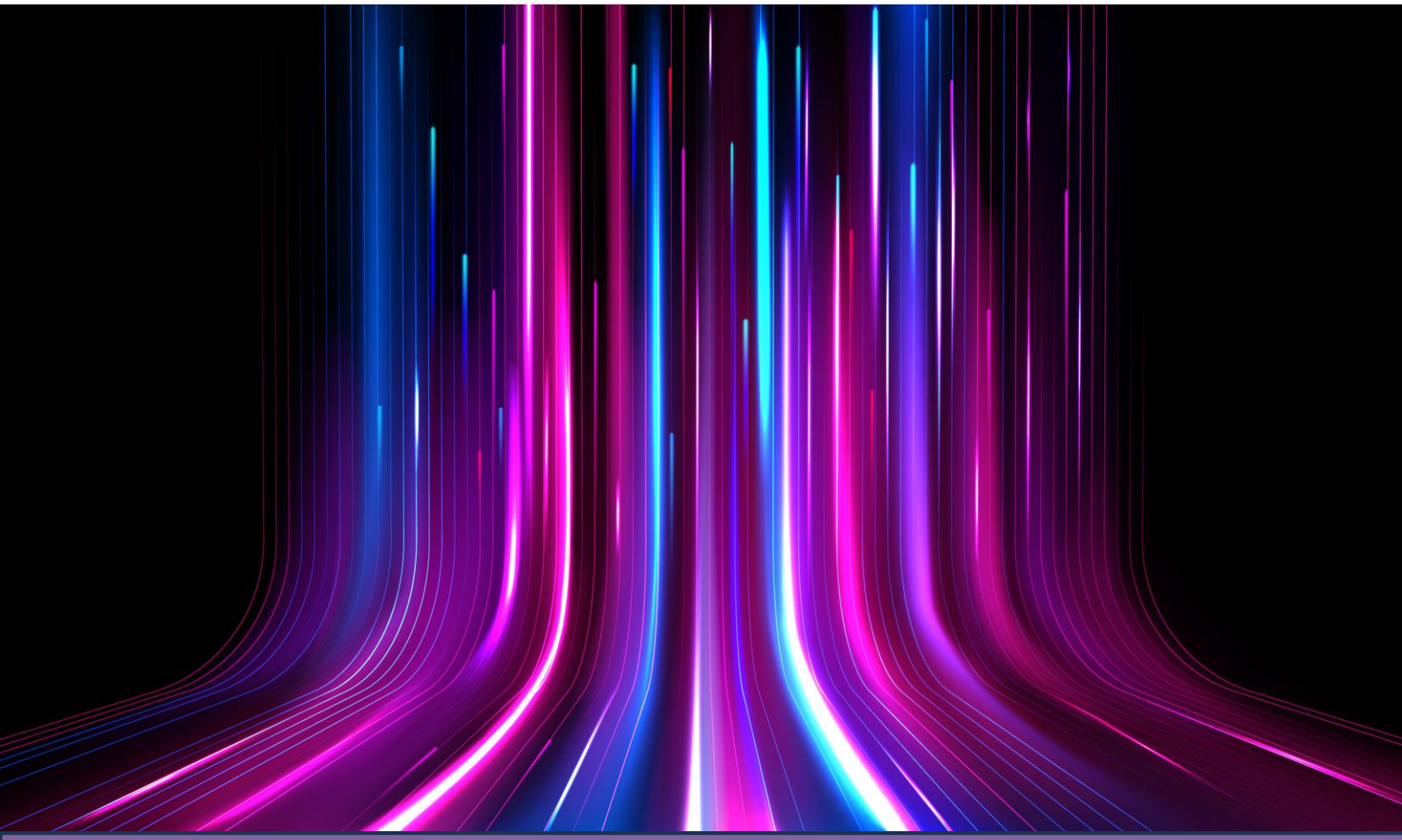
RadiGaMe Briefing



Forschungsethische Aspekte der Datenerhebung aus geschlossenen Gruppen auf Gaming-nahen Plattformen sowie Messenger-Diensten

Robert Pelzer, Tobias Weidmann

RADIGAME BRIEFING

Forschungsethische Aspekte der Datenerhebung aus geschlossenen Gruppen auf Gaming-nahen Plattformen sowie Messenger-Diensten

Titelbild: iStock klyaksun

Kontakt:
Leibniz-Institut für Friedens- und Konfliktforschung (PRIF) Baseler Straße 27–31
D-60329 Frankfurt am Main/Germany
E-Mail: radigame@prif.org
https://www.prif.org/
https://www.radigame.de

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

Der RadiGaMe-Forschungsverbund, wird vom Bundes-ministerium für Bildung
und Forschung (BMBF) im Rahmen der Fördermaßnahmen Zivile Si-cherheit -
Bedrohungen im digitalen Raum mit einer Laufzeit von 2023 bis 2026 gefördert.

Autoren:

Dr. phil. Robert Pelzer ist seit April 2014 als wissenschaftlicher Mitarbeiter im Bereich Sicherheit - Risiko – Kriminologie an der Technischen Universität in Berlin tätig. Seit 2019 leitet er den Forschungsbereich. Er koordiniert den Forschungsverbund RadiGaMe seit 2023.

Tobias Weidmann arbeitet seit Juli 2023 als wissenschaftlicher Mitarbeiter im Forschungsbereich „Sicherheit – Risiko – Kriminologie“. Er untersucht Radikalisierungsprozesse auf Gaming-Plattformen und Messenger Diensten und studierte Politikwissenschaften an der Freien Universität sowie Bildungsforschung an der Technischen Universität in Berlin.

Inhalt

Einführung 3
1 Forschungsethische Diskussion zu verdeckter Forschung 4
2 Ethische Dimensionen verdeckter Online-Radikalisierungsforschung 5
2.1 Verantwortung gegenüber dem Untersuchungsfeld 5
2.2 Verantwortung gegenüber Forscher:innen 12
2.3 Verantwortung gegenüber der Gesellschaft 13
3. Leitlinien für eine ethisch kontrollierte Forschungspraxis 14
3.1 Allgemeine Anforderungen 14
3.2 Verfahren zur Einzelfallprüfung 15
Literatur 23

Forschungsethische Aspekte der Datenerhebung aus geschlossenen Gruppen auf Gaming-nahen Plattformen sowie Messenger-Diensten

Robert Pelzer & Tobias Weidmann

EINFÜHRUNG

In RadiGaMe werden Kommunikations- und Interaktionsprozesse zwischen radikalisierten Nutzer:innen auf Gaming-nahen Plattformen sowie auf Messenger-Diensten beobachtet, erhoben und ausgewertet. Die Kommunikation von rechtsextremen Akteur:innen auf Plattformen wie Telegram oder Discord findet mit zunehmendem Radikalisierungsgrad in nach Außen geschlossenen Kommunikationsräumen statt, deren Zutritt kontrolliert wird. Diese Räume lassen sich nicht unter der Voraussetzung einer informierten Einwilligung der Nutzer:innen beforschen, da Forschenden in der Regel erhebliches Misstrauen entgegengebracht wird. Um Forschung zu ermöglichen, müssen sich Forschende unter Vortäuschung einer unverfänglichen Teilnehmenden-Rolle Zutritt verschaffen. Durch eine solche verdeckte Teilnahme und ggf. Datenergebung wird insb. die Vertraulichkeit der Kommunikation der Nutzer:innen verletzt. Sie stellt damit einen nicht unerheblichen Eingriff in die Persönlichkeitsrechte der in den Räumen kommunizierenden Personen dar. Demgegenüber steht jedoch ein erhebliches gesellschaftliches Interesse an der Erzeugung von wissenschaftlichen Erkenntnissen, die zur Problemlösung, d.h. Abwehr von demokratie- und sicherheitsgefährdenden Entwicklungen, beitragen. Es bestehen somit gegenläufige Interessen von Beforschten und Gesellschaft, die jeweils hochwertige ethische Güter berühren und gegeneinander abzuwägen sind, um zu einer ethischen Entscheidung zu gelangen.

Ziel des Briefings ist es, Leitlinien für eine ethisch kontrollierte Entscheidungsfindung hinsichtlich einer verdeckten Teilnahme und Datenerhebung in Online-Räumen im Feld der Radikalisierungsforschung, insbesondere aus Perspektive der qualitativen Sozialforschung, zu entwickeln. Nichtsdestotrotz lassen sich die hier aufgeführten prinzipiellen Vorschläge sicherlich auch auf quantitativ ausgerichtete Vorhaben anwenden. Hierzu werden im ersten Teil die forschungsethischen Dimensionen und Herausforderungen der Beforschung zugangsregulierter radikaler Räume erörtert. Im zweiten Teil werden Leitlinien für einen ethisch kontrollierten Forschungsprozess dargestellt. Im Mittelpunkt steht die Skizzierung eines Verfahrens, um das gesellschaftliche Interesse an der Forschung mit den schutzwürdigen Interessen der Beforschten abzuwägen und auf dieser Grundlage eine Einzelfallentscheidung über die verdeckte Teilnahme und Datenerhebung in einer Gruppe treffen zu können. Die im Folgenden dargestellten Überlegungen bilden einen vorläufigen Arbeitstand, der als Ausgangspunkt für weitere Diskussion dienen soll.

1 Forschungsethische Diskussion zu verdeckter Forschung

Die ethischen Aspekte verdeckter Forschung wurden in den Sozialwissenschaften bisher v.a. hinsichtlich der Methode der verdeckten teilnehmenden Beobachtung in der realen Welt diskutiert. Dabei besteht Einigkeit, dass alle Formen der teilnehmenden Beobachtung Elemente der Täuschung enthalten, etwa indem emotionale Beteiligung vorgespielt wird oder Fragen gestellt werden, von deren Zielsetzungen die Erforschten nichts ahnen (vgl. Hopf 2000: 593). Gegenstand heftiger Kontroversen in den Sozialwissenschaften war die Frage der Zulässigkeit einer verdeckten Beobachtung, bei der Akteure im Feld über die Identität der:des Forschenden über einen längeren Zeitpunkt hinweg getäuscht werden (zur Diskussion siehe allgemein: Bulmer 1980, 1982, spezifisch zur Kriminologie: Holdaway 1992, Wells 2004, Dodds 2004). Befürworter:innen der verdeckten Beobachtung verweisen auf die Ermöglichung von Forschung in verschlossenen Milieus, durch die die Forschung ihrer gesellschaftlichen Verantwortung gerecht werde. So argumentiert Lauder (2003), der verdeckt an rechtsextremen Aktivitäten teilnahm, dass der Zugang zu verschlossenen Milieus wie kriminellen Banden, radikalen politischen und religiösen Gruppen aber auch staatlichen Institutionen, oft nur hergestellt werden könne, wenn der:die Forschende eine unverfängliche Mitgliedschaftsrolle einnimmt. Auch würden Forschende nur in der Mitgliedschaftsrolle Zugang zu unverfälschten oder ansonsten unter Verschluss gehaltenen Informationen erhalten. Schließlich leiste Forschung auf Grundlage der ansonsten nicht zu erlangenden Forschungsergebnisse einen Beitrag zur Reduzierung destruktiven sozialen Verhaltens, politischer Gewalt, u.a. Demgegenüber argumentierten Gegner:innen der verdeckten Beobachtung mitunter, dass eine Beeinflussung des Untersuchungsfelds stattfinde, die sich nachträglich als Störvariable nur schwer neutralisieren lasse. Dem kann jedoch entgegengehalten werden, dass Forschende und Beforschte stets miteinander interagieren und sich somit auch wechselseitig beeinflussen, was nicht als Verzerrungsfaktor, sondern vielmehr als Zeichen für die ‚Natürlichkeit' der Untersuchung anzusehen sowie als eigenständiges soziales Phänomen zu betrachten und zu analysieren ist (vgl. Wolff 2000: 339). Gewichtiger scheint demgegenüber das Argument, dass bei verdeckten Beobachtungen nur fragile Arrangements zustande kommen können, bei denen stets Kontaktverlust und Entdeckung drohen und ein hoher Auffand für Informationskontrolle und Eindrucksmanagement nötig ist, der direkte Kommunikationen erschwert und damit die Möglichkeiten der Datenerhebung limitiert (vgl. Wolff 2000: 341).

Während man sich in der deutschsprachigen Soziologie in der Ablehnung verdeckter Beobachtung weitgehend einig ist (vgl. Hopf 2000: 592), wird sie im Ethik-Kodex der ASA weniger massiv abgelehnt. In seltenen Fällen könne demnach die Verbergung der Identität der Forschenden nötig sein, um Forschung überhaupt zu ermöglichen. Dabei dürften die Risiken für die Beforschten jedoch nur gering sein und eine institutionelle Ethikkommission oder, falls es keine solche gibt, einer anderen maßgeblichen Stelle mit Fachkenntnissen auf dem Gebiet der Forschungsethik, müsse dem Vorgehen zustimmen.[1]

[1] „On rare occasions, sociologists may need to conceal their identities in order to undertake research that could not practicably be carried out were they to be known as researchers. Under such circumstances, sociologists undertake the research if it involves no more than minimal risk for the research participants and if they have obtained approval to proceed in this manner from an institutional review board or, in the absence of such boards, from another authoritative body with expertise on the ethics of research. Under such circumstances, confidentiality must be maintained unless otherwise set forth in 11.02(b)." (12.05d, Codes of ethics der American Sociological Association)

Auch in der Online-Forschung wird das Vermitteln der eigenen Identität als Forschende:r sowie des Forschungsvorhabens, etwa durch Informationen auf dem eigenen Nutzer:innenprofi, als „Voraussetzung für eine nicht schädigende Online-Forschung, die mögliche Risiken für die Untersuchungssubjekte vermeidet" (Heise/Schmidt 2014: 523) gesehen. So empfehlen Heise/Schmidt (2014), dass die Beobachtung offen geschehen sollte, sofern „keine gravierenden methodologischen Gründe dagegen sprechen". Im Falle verdeckter Beobachtung sollten die Nutzer:innen vor der Veröffentlichung der Ergebnisse in jedem Falle informiert werden.

Zusammenfassend lässt sich feststellen, dass ethische Aspekte verdeckter Online-Forschung bislang nicht ausführlich und umfassend diskutiert wurden und entsprechende Leitlinien für die Forschungspraxis fehlen (vgl. Demant/Moretti 2024). Dies gilt insbesondere für das Feld der Online-Radikalisierungs- und Extremismusforschung, dessen Besonderheiten in bisherigen forschungsethischen Leitlinien nicht Rechnung getragen wird (vgl. Conway 2021).

2 Ethische Dimensionen verdeckter Online-Radikalisierungsforschung

Bei der Beforschung zugangsregulierter radikalisierter Räume stellen sich verschiedenartige ethische Herausforderungen, die im Folgenden entlang der drei forschungsethischen Dimensionen von Verantwortung erörtert werden: (1) die Verantwortung gegenüber dem Untersuchungsfeld (externe Verantwortung), (2) die Verantwortung gegenüber Forschenden (interne Verantwortung) sowie (3) die Verantwortung für das Wohlergehen der Gesellschaft (gesellschaftliche Verantwortung).

2.1 Verantwortung gegenüber dem Untersuchungsfeld

Die externe Verantwortung bezieht sich auf das Untersuchungsfeld als Ganzes und die jeweils untersuchten Subjekte. Zentrale Aspekte hier sind die Freiwilligkeit der Teilnahme, die informierte Einwilligung, der Schutz der Vertraulichkeit der Beforschten sowie der Grundsatz der Nicht-Schädigung.

Informierte Einwilligung und Zugangshürden ins Feld radikalisierter Akteur:innen

Auch öffentlich verfügbare Kommunikationsdaten von Nutzer:innen auf Social Media-Plattformen sind in der Regel personenbezogene Daten, über deren Verwendung sie selbst bestimmen dürfen.[2] Eine informierte Einwilligung der Nutzenden ist daher nicht aus forschungsethischer Sicht anzustreben und bildet ebenso die datenschutzrechtlich bestmögliche Legitimation der geplanten Datenerhebung und -verarbeitung. Die zu beforschenden radikalisierten Nutzer:innen stehen Forschenden jedoch in der Regel äußerst skeptisch gegenüber und werden aus diesem Grunde nur in den seltensten Fällen dazu bereit sein, einer Datenerhebung zu Forschungszwecken zuzustimmen (vgl. Sold/Junk 2021).

Dabei wäre zunächst festzustellen, dass der Feldzugang zu abweichenden oder delinquenten Milieus grundsätzlich eine große Herausforderung bildet, da Forschende mit teils erheblichem Misstrauen der Akteur:innen im Feld hinsichtlich ihrer nicht-schädigenden Absichten konfrontiert sind. Das Misstrauen der Akteur:innen gründet auf dem Wissen um die gesellschaftliche Etikettierung und Missbilligung ihrer Lebenswelten als abweichend und

[2] Auch unter einem Pseudonym veröffentlichte Daten sind personenbezogen, da die natürliche Person unter Zuhilfenahme weiterer Informationen (z.B. IP-Adresse, weitere Bestandsdaten der Plattformbetreiber) möglicherweise identifiziert werden kann (RatSWD 2023: 20). Gleichwohl wäre festzustellen, dass es auf bestimmten Plattformen wie Telegram selbst Sicherheitsbehörden häufig nicht möglich ist, die hinter einem Nutzer:innennamen stehende Person zu identifizieren.

damit verbundenen Erfahrungen der Stigmatisierung. Bei Formen politisch oder religiös begründeter Devianz wird Misstrauen zusätzlich durch eine starke ideologisch begründete Ingroup-Outgroup-Grenzziehung verstärkt. Die Umwelt außerhalb der eigenen Gruppe oder Szene wird überwiegend als feindlich wahrgenommen. Forschungseinrichtungen sind mitunter Teil des Feindbildes. So deuten rechtsextreme Akteur:innen wissenschaftliche Einrichtungen als Bestandteil eines Regimes zur Durchsetzung von „Multi-Kulti-Ideologien".

In realweltlichen Forschungssituationen kann dieses Misstrauen durch einen auf persönlichem Kontakt basierenden Vertrauensbau in Einzelfällen durchaus überwunden werden, so dass es mit hohem Aufwand gelingen kann, Akteur:innen zur Teilnahme an kontrollierten Forschungssettings wie Interviews oder Gruppendiskussionen zu gewinnen. Die Erfahrung zeigt dabei, dass die Erfolgschancen mit zunehmendem Radikalisierungsgrad sinken. Dabei ist die Zugangshürde zu einer teilnehmenden Beobachtung oder gar Tonbandaufzeichnung von „natürlichen" Interaktions- und Kommunikationsprozessen in Gruppen wesentlich höher, da dadurch ein tiefgreifender und gewissermaßen (durch fehlendes Eindrucksmanagement) unverfälschter Einblick in die Innenwelt gegeben wird. Dass (hoch)radikalisierte Akteur:innen Forschenden einen solchen Zugang gewähren, scheint nur im Grenzfall einer bestehenden Zugehörigkeit des Forschenden zum Untersuchungsfeld realisierbar.

Das für einen offenen Feldzugang erforderliche Vertrauen lässt sich im Kontext von Online-Forschung wesentlich schwieriger herstellen. Zwar ist ein Vertrauensaufbau zu Akteur:innen im Feld grundsätzlich auch durch Nutzung von digitalen Kommunikationsmedien wie etwa Messenger-Diensten möglich. Vertrauen lässt sich hier jedoch nicht im gleichen Maße wie im Kontext ko-präsenter Interkationen aufbauen. Dies gilt sowohl für die Beziehung zwischen Forschenden und Beforschten, als auch für die Beziehungen zwischen den zu beforschten Teilnehmenden an zugangsregulierten Online-Gruppen. Denn sofern sich die Beforschten untereinander nicht persönlich kennen, was dem Anschein nach häufig der Fall ist, können sie ihr Vertrauen nur auf eine den Interaktionspartnern jeweils zugeschriebene Gesinnung stützen. Dadurch ist die feldzugangsgewährende Funktion von Gatekeepern in der Offline-Forschung, die den:die Forschende an ihren persönlichen Netzwerken partizipieren lassen, eingeschränkt. Denn der:die Gatekeeper:in kann zum einen für einen:eine Forschende, zu der:dem er:sie keinen realweltlichen Kontakt hat, nur schwer seine:ihre „Hand ins Feuer legen". Zum anderen ist das Vorschussvertrauen des:der Gatekeeper:in aufgrund der fragilen, auf Gesinnung gestützten Vertrauensverhältnisse in anonymen Online-Gruppen weniger Wert. Gleichwohl sind bestimmte digitale Räume durchaus hierarchisch strukturiert, so dass ein offener Zugang über Gatekeeper zunächst immer geprüft werden solle, bevor sich für eine verdeckte Teilnahme als Ultima Ratio entschieden wird.

Gleichzeitig bildet ein gelungener Vertrauensaufbau auch in der Online-Forschung eine notwendige Voraussetzung für einen offenen Feldzugang zu zugangsregulierten Gruppen. Denn zugangsregulierte digitale Räumen wie (geschlossene) Telegram-Gruppen oder Discord-Server sind mit realweltlicher Intra-Gruppen-Kommunikation in der Hinsicht vergleichbar, dass Akteur:innen in einem geschützten Raum unter Gleichgesinnten kommunizieren und ihre im Außenbezug potentiell kompromittierenden radikalen Anschauungen, offen artikulieren. Zwar kommunizieren die Akteur:innen hier im Unterschied zur realen Welt gewöhnlich unter einem Pseudonym, wodurch die persönlichen Risiken, dass das durch Forschende registrierte Online-Verhalten negative Konsequenzen für die Person in der realen Welt nach sich zieht, deutlich abgeschwächt sind. Das individuelle Risiko bleibt aber grundsätzlich bestehen. Hinzu tritt das Risiko, dass die von Gruppenteilnehmenden geäußerten Inhalte negative Auswirkungen auf das Untersuchungsfeld insgesamt haben könnten,

etwa, dass es durch die Forschungsergebnisse zu einer verstärkten strafrechtlichen Kontrolle oder zu Löschaktivitäten von Plattformbetreibern kommt. Dieses Argument wird dadurch verstärkt, dass in entsprechenden Online-Räumen in manchen Fällen die vorausgegangene, eventuell strafbare, Kommunikation für Forschende noch sichtbar und nachvollziehbar ist. Während in der realweltlichen Teilnahme entsprechend strafbares Verhalten während der Anwesenheit des:der Forscher:in leichter unterlassen werden kann, was eine eventuelle Bereitschaft der Teilnahme im Vergleich zur Online Kommunikation erleichtern dürfte. Ein offener Feldzugang zu zugangsregulierten Räumen scheint vor diesem Hintergrund wie in der realen Welt nur in Grenzfällen realistisch zu sein.

Informierung der Nutzer:innen über Datenerhebung

Lässt sich ein Feldzugang in der Online-Radikalisierungsforschung in der Regel nicht unter der Voraussetzung einer informierten Einwilligung der beforschten Nutzer:innen realisieren, wäre aus forschungsethischer Sicht gleichwohl zu prüfen, ob die Nutzer:innen nach Abschluss der Feldphase über das konkrete Forschungsvorhaben, in dessen Rahmen Kommunikationsdaten erhoben wurden, informiert werden können.

Dabei wäre davon auszugehen, dass die Beforschten zunächst keine Kenntnis darüber haben, dass sie beforscht werden bzw. wurden, da die Datenerhebung verdeckt erfolgt und in den publizierten Ergebnissen zudem aus ethischen und datenschutzrechtlichen Gründen zwingend die faktische Anonymität der Beforschten sicherzustellen ist. Durch die nachträgliche Informierung würde daher ein Eingriff in das Feld erfolgen, mit dem sich verschiedene Risiken verbinden. Zunächst könnte die nachträgliche Informierung der Beforschten dazu führen, dass diese davon ausgehen, dass sie nun auch Sicherheitsbehörden gegenüber bekannt sind, was zu einem verstärkten Gefühl des Überwachtwerdens und daraus resultierenden Verhaltensveränderungen (etwa „chilling effects“) führen kann. Bilden ablehnende Reaktionen des Feldes auf seine Beforschung den maßgeblichen Erwägungsgrund für eine Datenerhebung ohne Einwilligung der Nutzer:innen, so muss im Falle einer nachträglichen Informierung der Nutzer:innen mit entsprechenden negativen Reaktionen des Feldes gerechnet werden. Eine diesbezügliche Folgenabschätzung müsste berücksichtigen, dass Wissenschaftler:innen verstärkten Anfeindungen im Feld ausgesetzt werden, was den Feldzugang weiter erschwert. Die Forschenden selbst würden sich dem Risiko persönlicher Anfeindungen aussetzen, die über Hassmails, bis hin zu Drohungen und im schlimmsten Fall tätlichen Angriffen reichen können.

Darüber hinaus müsste eine Abwägung hinsichtlich der Durchführbarkeit der Informierung vorgenommen werden, was angesichts einer häufig hohen Anzahl von Anwesenden in entsprechenden Kommunikationsräumen mit einem sehr hohen Aufwand seitens der Forscher:innen einher gehen würde.

Zusammenfassend lässt sich feststellen, dass eine nachträgliche Informierung erhebliche Risiken birgt, die insbesondere mit Blick auf die Dimension interner Verantwortung nicht tragbar wären.

Vertraulichkeit

Der forschungsethische Grundsatz der Vertraulichkeit bezieht sich auf den Schutz der persönlichen Daten und Informationen der Teilnehmenden. Dieser Grundsatz verlangt, dass Forschende die Identität und persönlichen Informationen der Teilnehmenden schützen und sicherstellen, dass diese Dritten nicht unbefugt zugänglich gemacht oder veröffentlicht werden. Der Schutz der Vertraulichkeit ist in besonderer Weise tangiert wenn Forschende sich unter Vortäuschung der Rolle eines unverfänglichen Teilnehmenden einem zugangs-

regulierten digitalen Raum beitreten, in welchem die Teilnehmenden Informationen bewusst nur mit einem nach bestimmten Kriterien ausgewählten Kreis von Nutzer:innen austauschen wollen. „Vertraulich" sind alle Informationen, die die Privatsphäre einer Person betreffen und nur mit einem bestimmten Empfänger:innenkreis geteilt werden sollen. Dazu gehören auch politische Anschauungen[3]. Die Teilnehmenden geben in zugangsregulierten Gruppen ggf. Informationen preis, die sie Personen außerhalb der Gruppe, einschließlich Forschenden, nicht preisgeben würden. Die Verwendung dieser Informationen ohne Zustimmung der Betroffenen stellt eine Vertraulichkeitsverletzung dar, deren Grad jedoch erheblich variieren kann abhängig von den Privatheitserwartungen der Teilnehmenden, ihrem Anonymitäts- bzw. Pseudonymitätsgrad, der Gruppengröße sowie der Sensibilität der geteilten Informationen. In dem forschungsethischen Abwägungsprozess muss insbesondere berücksichtigt werden, inwiefern sich die Vertraulichkeit der unter Täuschung erlangten Informationen im Außenverhältnis gegenüber unbefugten Dritten gewährleisten lässt. Hier ist im Rahmen des Datenschutzes zu prüfen, welche Risiken für die Betroffenen bestehen, dass Unbefugte trotz Umsetzung eines höchstmöglichen technischen und organisatorischen Schutzniveaus a) Zugriff auf die erhobenen Daten erlangen und b) einen Personenbezug der erhobenen Daten (wieder)herstellen können. Bei Daten zum Radikalisierungsgeschehen von Nutzer:innen geschlossener Gruppen muss grundsätzlich ein hypothetisches Interesse von Sicherheitsbehörden an Daten unterstellt werden. Maßstab der Risikoabschätzung sollte daher stets das Szenario einer Beschlagnahme von Forschungsdaten durch sicherheitsbehördliche Akteure sein.

Für die Risikoabschätzung, aber auch mit Blick auf die Frage, ob die erhobenen Daten als vertraulich einzustufen sind, ist zuallererst zu klären, ob die Daten einen Personenbezug aufweisen. Im hypothetischen Falle einer vollständigen Anonymität der (aller) in einer geschlossenen Gruppe kommunizierenden Nutzer:innen hätten die erhobenen Daten keinerlei Personenbezug und wären damit nicht mehr im Sinne der Vertraulichkeit schutzwürdig. In der Forschungspraxis kann eine vollständige Anonymität jedoch nie angenommen werden, da im Einzelfall stets unklar bleibt, ob Sicherheitsbehörden einer Personenidentifizierung mit erheblichem Aufwand unter Hinzuziehung weiterer Informationen nicht aktuell oder in naher Zukunft doch gelingen könnte. Auch eine faktische Anonymität pseudonym kommunizierender Nutzer:innen kann in der Forschungspraxis nicht angenommen werden. Denn hierzu müsste geprüft werden, ob eine Personenidentifizierung für Sicherheitsbehörden faktisch, d.h. mit aktuell zur Verfügung stehenden Ressourcen und Techniken nicht möglich wäre.[4] Zwar berichten Praktiker:innen aus Sicherheitsbehörden, dass eine Identifizierung pseudonym agierenden radikalisierter Nutzer:innen auf Plattformen wie Telegram in vielen Fällen oder gar im Regelfall faktisch nicht möglich sei, da Plattformbetreiber Bestandsdaten entweder gar nicht erst übermitteln oder diese nicht ermittlungsdienlich sind, etwa weil Nutzer:innen ihre IP-Adresse verschleiern. Da eine Nutzer:innenidentifikation im Einzelfall möglich bleibt und nicht abschätzbar ist, welche Nutzer:innen und Inhalte davon betroffen sein könnten, kann lediglich eine Pseudonymität der Nutzer:innen angenommen werden. Entsprechend müssen die in geschlossenen Gruppen kommunizierten Inhalte als potenziell personenbeziehbar und damit vertraulich angesehen werden.

[3] Diese unterliegen im Sinne des Art. 9 der DSGVO als besondere Kategorien personenbezogener Daten einem besonderen Schutz.

[4] Für eine Nutzer:innenidentifikation können Sicherheitsbehörden ggf. auf Informationen aus Bestandsdaten der Plattform- und/oder Internetserviceprovider zurückgreifen, aber auch auf Erkenntnisse aus OSINT-Recherchen zu Aktivitäten der:des zu identifizierenden Nutzer:in auf anderen Plattformen.

Für die Bewertung des Vertraulichkeitsgrades der in zugangsregulierten Gruppen geteilten Informationen wird vorgeschlagen zwei Kriterien heranzuziehen: Erstens der Privatheitsbezug der kommunizierten Inhalte und zweitens die in Hinblick auf den Empfänger:innenkreis der in einem konkreten Kommunikationsraum geteilten Inhalte bestehenden Privatheitserwartungen von Nutzer:innen.

Der Privatheitsbezug lässt sich nach dem vom Bundesverfassungsgericht entwickelten Drei-Sphärenmodell des allgemeinen Persönlichkeitsrechts differenzieren in Intimsphäre, Privatsphäre und Sozialsphäre (vgl. Poscher 2010). Die *Intimsphäre* betrifft die innerste Gedanken- und Gefühlswelt sowie höchstpersönliche Informationen, wie beispielsweise zum Gesundheitszustand oder zum Sexualleben, also all jene Informationen, die ein Individuum, wenn überhaupt, nur mit engen Vertrauten teilt. Die *Privatsphäre* bezieht sich auf Informationen über das persönliche Leben, die Individuen gewöhnlich vor der Öffentlichkeit schützen möchten, etwa über das Familienleben, Hobbies, aber auch über persönliche politische und religiöse Überzeugungen. Die dritte Sphäre, die *Sozialsphäre*, bezeichnet Aktivitäten einer Person, die gewöhnlich von außen wahrnehmbar sind, z.B. soziale Kontakte, Kinobesuche, o.ä., die jedoch keine bewusste Hinwendung zur Öffentlichkeit darstellen. Auch die nach außen wahrnehmbare Teilnahme an weltanschaulichen Gruppen und die damit verbundene Zugehörigkeit zu einer bestimmten Kategorie von Ideologie bzw. Weltanschauung wäre demnach als Teil der Sozialsphäre zu betrachten. Welche Informationen welcher Sphäre angehören, hängt aus soziologischer Sicht von lebensweltspezifischen Praktiken und Gewohnheiten der Untersuchungsgruppen ab. Für die Betrachtung der Online-Kommunikation radikalisierter Nutzer:innen gilt es daher zu unterscheiden, inwiefern die Nutzer:innen in einer bestimmten Online-Szene ihre Gruppenzugehörigkeit gewöhnlich nach außen tragen. Für den hier verhandelten Fall zugangsregulierter Online-Gruppen nehmen wir jedoch an, dass die dort geteilten Haltungen zu politischen und weltanschaulichen Themen der Privatsphäre angehören, da sie über die bloße Zugehörigkeit zu einer Ideologie hinaus auch Aufschluss über individuelle Ausprägungen weltanschaulicher Positionen geben, die von den Individuen bewusst der Sozialsphäre entzogen werden.

Die Privatheitserwartungen hängen davon ab, ob Nutzer:innen eine vertrauliche Gruppenkommunikation erwarten können. Golla et al. (2019: 246) folgend ist dafür maßgeblich, ob der Personenkreis, dem die geteilten Informationen zugänglich sind, faktisch beschränkt wird. Die Privatheiterwartungen sind demnach umso geringer einzustufen, je leichter der Zugang zu einem digitalen Kommunikationsraum möglich ist. Sofern die Zugangsbeschränkung nur technischer Natur ist, handele es sich demnach um einen offenen, nicht zugangsregulierten Raum mit geringen Privatheitserwartungen. Das bedeutet, dass in der Regel durch einen einfachen Registrierungs- bzw. Anmeldeprozess die Daten durch alle Nutzer:innen der jeweiligen Social Media-Plattform eingesehen werden können (ebd.: 242). Auch Gruppen, denen jeder Mensch durch einen Zugangslink beitreten kann sind nach diesem Verständnis offene Gruppen, selbst wenn der Zugangslink schwer auffindbar ist, da er nur in ausgewählten öffentlich einsehbaren Räumen gepostet wurde. Da faktisch allen Nutzer:innen Zugang gewährt wird, können Nutzer:innen nicht in einen effektiv geschützten Kommunikationsraum vertrauen.

In welchem Ausmaß Nutzer:innen eine vertrauliche Gruppenkommunikation erwarten können, hängt nun davon ab, nach welchen Kriterien der Zugang zum Online-Raum reguliert wird und wie effektiv diese Kriterien überprüft werden. In radikalen Gemeinschaften oder Milieus vermittelt sich Vertrauen zunächst durch die Zugehörigkeit zur Ingroup, die auf geteilten Überzeugungen, Werten und Einstellungen, also auf einer bestimmten Gesinnung basiert. In Hinblick auf die Vertraulichkeitserwartungen geht es also darum, wie effektiv

das Vorliegen einer entsprechenden Gesinnung überprüft wird. Anhand unserer Explorationen in Telegram-Gruppen im Projekt RadiGaMe lassen sich diesbezüglich vier Stufen unterscheiden:

- Stufe 1: Während des Zugangsprozesses wird eine kurze Interaktion nötig, in deren Zuge z.B. eine inhaltliche Frage schriftlich beantwortet werden soll. Dabei kann es sich auch um eine Frage zur Motivation handeln. Abgefragt wird somit eine Selbst-Kategorisierung der:des Anfragenden, die jedoch von Gruppenmitgliedern/Administrator:innen , nicht weiter überprüft wird.
- Stufe 2: Im Unterschied zu Stufe 1 wird die Motivation bzw. Szenezugehörigkeit der:des Zutrittsuchenden im Rahmen einer dialogischen Interaktion über ggf. mehrere Zyklen, etwa durch einen Austausch von Textnachrichten, überprüft. Es erfolgt dabei eine Abfrage von allgemeinen Einstellungen oder Wissenselementen mittels standardisierter Fragen, jedoch keine eingehende Prüfung der Gesinnung o.ä. Um Zutritt zu erhalten ist gleichwohl der Rückgriff auf eine legendierte Erzählung und somit ein höheres Maß an Täuschung als in Stufe 1 erforderlich.
- Stufe 3: Auf dieser Stufe findet eine eingehende individuelle Prüfung der Interessen und Gesinnung der:des Anfragenden statt, die eine aktive und umfangreiche Täuschung des Prüfenden mithilfe der Legende notwendig macht. Die Interaktion erfolgt etwa im Rahmen eines Audio-Calls, bei dem die Pseudonymität des:der Zutrittsanfragenden jedoch gewahrt bleibt. Eine vergleichbare Zugangshürde besteht, wenn eine bereits bestehende Bekanntschaft mit positiven Erfahrungen aus anderen Online-Räumen Voraussetzung für die Teilnahme ist. In diesem Fall müsste in vorherigen Räumen durch aktive Teilnahme eine Zugehörigkeit zur Ingroup vorgetäuscht werden, was einer umfangreichen legendierten Erzählung in einer Prüfsituation gleichkommt.
- Stufe 4: Auf dieser Stufe beinhaltet die individuelle Prüfung auch eine Offenlegung der personalen Identität der:des Anfragenden, z.B. durch Vorzeigen eines Personalausweises oder durch eine Befragung in einem Video-Call, in dessen Rahmen der:die Anfragende ihr:sein Gesicht zeigen muss. Es kommt also zu einer Entpseudonymisierung der:des Anfragenden.

Auf der ersten Stufe lassen sich für durchschnittlich-rationale Nutzer:innen nur geringe Privatheitserwartungen ableiten, da das Vorliegen einer bestimmten Gesinnung nicht überprüft und der Empfänger:innenkreis damit nicht effektiv begrenzt wird. Nutzer:innen müssen also damit rechnen, dass sich unter den Teilnehmenden auch Nicht-Szeneangehörige wie Journalist:innen, Wissenschaftler:innen, Sicherheitsbehörden oder politischer Gegner:innen befinden. Auf den Stufen zwei und drei wird demgegenüber durch die individuelle Gesinnungsprüfung ein Raum mit mittleren bis hohen Vertraulichkeitserwartungen konstituiert, der sich als privater Raum charakterisieren lässt, da die Inhalte nur mit einem nach dezidierten Kriterien ausgewählten Empfänger:innenkreis geteilt werden sollen. Die pseudonyme Gesinnungsprüfung begründet jedoch noch keine sehr hohen Vertraulichkeitserwartungen, da die Gesinnung unter Bedingungen der Pseudonymität mit überschaubarem Aufwand vorgespielt werden kann. Sehr hohe Vertraulichkeitserwartung wären demnach erst bei der vierten Stufe anzunehmen.

Zusammenfassend lässt sich das Ausmaß der Vertraulichkeitsverletzung von verdeckter Forschung in zugangsregulierten radikalisierten Räumen als Produkt aus dem Privatsphärebezug der kommunizierten Inhalte sowie den Vertraulichkeitserwartungen der Teilnehmenden ergeben, beschreiben.

Nicht-Schädigung

Der Grundsatz der Nicht-Schädigung bedeutet, dass durch die Teilnahme an einem Forschungsprojekt oder die Ergebnisse der Forschung als solche keine negativen Folgen für die schutzwürdigen Interessen der beforschten Akteur:innen sowie für die Akteur:innen im Untersuchungsfeld insgesamt entstehen dürfen. Schutzwürdig sind dabei nicht nur die Freiheitsrechte individueller Akteur:innen, sondern auch die demokratischen Artikulationsmöglichkeiten für politischen Protest insgesamt, was grundsätzlich auch die Artikulation von extremen politischen Inhalten einschließt, solange diese von der Meinungsfreiheit gedeckt sind. Diese demokratischen Freiheitsrechte gelten selbstredend auch für rechtsextreme Akteur:innen und dürfen auch hier nur unter engen gesetzlichen Voraussetzungen eingeschränkt werden. Der Schutz demokratischer Freiheitsrechte kann jedoch in einem Spannungsverhältnis zu extremismuspräventiven, demokratisch-zivilgesellschaftlichen Verwertungsinteressen der Radikalisierungsforschung stehen, da die Prävention und Bekämpfung des Rechtsextremismus immer auch auf eine Einschränkung der politischen Entfaltungsmöglichkeiten rechtsextremer Akteur:innen abzielt, bspw. durch die öffentliche Stigmatisierung von rechtsextremen Akteur:innen oder ein repressives Protest Policing. Aus forschungsethischer Sicht gilt es zunächst, dieses Spannungsverhältnis mit Blick auf die konkreten Ziele und Verwertungsinteressen der Forschung transparent zu machen. Dabei gilt es zu reflektieren bzw. abzuschätzen, welche Folgen die angestrebte aber auch eine nicht intendierte Verwertung der Forschungsergebnisse durch Praxisakteur:innen für die Freiheitsrechte der Akteur:innen im Untersuchungsfeld haben könnten. Beispielsweise könnten die Forschungsergebnisse zu einem stärker risikobasierten Umfang mit rechtsextremen Akteur:innen beitragen, durch den Eingriffsmaßnahmen weiter in das Vorfeld von Straftaten vorverlagert werden. Hier wäre zu reflektieren, inwiefern eine solche Praxis „chilling effects“ mit sich bringt, in deren Zuge rechte Akteur:innen bestimmte Meinungen, die im Rahmen der Meinungsfreiheit zulässig sind, in der Öffentlichkeit zunehmend weniger äußern, da sie Angst vor Strafverfolgung oder anderen missbilligenden Reaktionen haben. Diese grundrechtlich negativen Folgen müssten mit demokratisch-zivilgesellschaftlich legitimen Interessen der Prävention und Bekämpfung des Rechtsextremismus abgewogen werden.

Auf individueller Ebene geht es bei Nicht-Schädigung um Risiken für Freiheitsrechte der konkret beforschten Subjekte. Es gilt fallangemessene Maßnahmen zu treffen, um diese Risiken so weit wie möglich zu minimieren. Aus forschungsethischer Sicht ist dabei von Bedeutung, dass die schutzwürdigen Interessen der Beforschten unabhängig von ihrer Gesinnung allgemeine Gültigkeit haben, d.h. dass auch eine antidemokratische bis menschenverachtende Haltung der Beforschten nicht zu Beeinträchtigungen der zugestandenen Schutzwürdigkeit und darauf bezogenen praktischen Schutzmaßnahmen führen darf. So darf der Schutz der Vertraulichkeit nur unter engen ethischen Maßstäben aufgehoben werden. Fraglos ist dabei zunächst die gesetzliche Pflicht zur Anzeige geplanter Straftaten.[5] Gerade im Bereich der Online-Radikalisierung können Forschende jedoch mit strafbaren Äußerungsdelikten oder nicht strafrechtlich aber möglicherweise für die Gefahrenabwehr relevanten Hinweisen auf eine gewaltorientierte Radikalisierung konfrontiert werden, die jeweils einer gesetzlichen Anzeigenpflicht nicht unterliegen.

Eine Meldung von Äußerungsdelikten (ohne „Gefahrenüberhang“) scheint ethisch grundsätzlich fragwürdig, auch dann, wenn die Daten aus offen zugänglichen Kommunikationsräumen erhoben wurden. Denn es ist nicht Aufgabe der Wissenschaft, Strafverfolgungsbehörden bei der Identifikation und Aufklärung von Straftaten zu unterstützen, sondern das

[5] Insb. die Anzeige von geplanten Straftaten nach § 138 StGB. Siehe dazu RatSWD 2023-

Radikalisierungsgeschehen, aus dem Straftaten resultieren, zu ergründen. Dazu sind strafbare Äußerungen im Feld der Radikalisierung ein systematisches Phänomen. Würden Wissenschaftler:innen diese Äußerungen methodisch kontrolliert erfassen, bewerten und für Strafverfolgungsbehörden dokumentieren („sichern"), könnten sie ihrer eigentlichen Arbeit nicht mehr nachkommen. Gleiches gilt für die Unterstützung der Gefahrenabwehr bzw. -aufklärung. Sofern Hinweise auf konkrete Gefahren (etwa geplante Gewaltakte) vorliegen, sollte eine Meldung erwogen werden. Viel häufiger sind Forschende aber mit Äußerungen von Nutzer:innen konfrontiert, die auf eine bestehende oder sich entwickelnde gewaltorientierte Radikalisierung hindeuten könnten. Um zu entscheiden ob dies der Fall ist, müssten individuelle Risikoeinschätzungen (Prognosen) vorgenommen werden, die wiederum weiterführende personenbezogene Recherchen zu Nutzer:innen erforderlich machten. Die Erforschung eines solchen ‚Gefahrenvorfelds' ist eine Aufgabe von Sicherheitsbehörden, die Forschende nicht leisten können. Im Falle von konkreten Gefahren bzw. aus Sicht der Forschenden konkretem Warnverhalten für Gewalthandlungen sollte eine Meldung des Sachverhalts zum Gegenstand einer ethischen Entscheidungsfindung gemacht werden, bei der das Risiko für eine Menschenleben gefährdende Straftat mit den Risiken für die Forschung (etwa die Löschung einer Gruppe oder eines Servers als Folge von Ermittlungsmaßnahmen) und Risiken für schutzwürdige Belange der im Falle von Maßnahmen Betroffenen abgewogen werden.

2.2 Verantwortung gegenüber Forscher:innen

Eine offene Beforschung radikalisierter Kommunikationsräume, bei der Forschende ihre Identität und ihr Forschungsanliegen den Nutzer:innen kundtun kann erhebliche Risiken bergen, sofern der Person und ihrem Anliegen vom Untersuchungsfeld feindliche Absichten zugeschrieben werden (Franzke et al. 2020: 11f). Forschende und ihre Einrichtung müssten dann mit Belästigungen, im schlimmsten Falle Drohungen rechnen. Dies gilt sowohl für die Beforschung von offenen als auch zugangsregulierten Kommunikationsräumen. Sofern ein offener Zugang erwogen wird, gilt es aus forschungsethischer Sicht das Risiko für die Forschenden vorab im Sinne einer Prognose der Reaktionen der Akteur:innen auf das Forschungsanliegen und die Forschenden abzuschätzen.

Im Falle verdeckter Forschung in zugangsregulierten Gruppen sind die Forschenden zwar durch ihre Legende geschützt. Im Falle des ‚Auffliegens' ihrer Legende würden Forschende jedoch einem weitaus höheren Risiko von Anfeindungen und Bedrohungen als im oben geschilderten Szenario ausgesetzt werden, da sie nun als „Spitzel" bzw. „Verräter" gelten. Auch bestehen Risiken für andere Forschende der Einrichtung oder Radikalisierungsforschende allgemein, die mit dem Forschungsvorhaben oder der Forschungsagenda assoziiert werden. Da hier potentiell gewaltorientierte Akteur:innen beforscht werden, muss neben Drohungen im schlimmsten Fall auch mit Gewalthandlungen gerechnet werden. Unter diesem Gesichtspunkt ist eine verdeckte Beforschung entsprechender Räume forschungsethisch nur dann vertretbar, wenn durch technische und organisatorische Maßnahmen sichergestellt werden kann, dass Forschende im Falle des „Auffliegens" ihrer Legende faktisch anonym bleiben. Dies ist nur bei zugangsregulierten Räumen bis zur Stufe 4 (siehe oben) möglich.

Um die faktische Anonymität der Forschenden gegenüber dem Untersuchungsfeld sicherzustellen müssen mindestens folgende technisch-organisatorische Maßnahmen ergriffen werden: Zunächst darf der genutzte Forschungsaccounts weder öffentlich noch für „Freunde" einsehbare Informationen erhalten, die eine „Spur" zur forschenden Person und ihrer Einrichtung aufweisen. Auch die Anmeldedaten dürfen keine Hinweise auf die Person des:der Forschenden beinhalten. Zudem ist es erforderlich, dass die genutzte Internetver-

bindung durchgehend mittels VPN-Client vor einer Rückverfolgung der IP-Adresse geschützt wird. Des Weiteren muss vor der Veröffentlichung von Ergebnissen die Verwendung von Originalzitaten sorgfältig hinsichtlich eines möglichen Risikos der Reidentifikation der Nutzer:innen oder anderweitiger Rückschlüsse auf Datenquellen geprüft werden. Besteht das Risiko einer Reidentifikation der beforschten Nutzer:innen wäre die faktische Anonymität der Forschenden gegenüber dem Untersuchungsfeld gefährdet, da auch diese die Publikation lesen und Rückschlüsse auf eine verdeckte Beforschung ihrer Online-Gruppe ziehen könnten.

Eine weitere Dimension der internen Verantwortung betrifft den Schutz der psychosozialen Gesundheit der verdeckt online Forschenden. Dabei geht es insbesondere um Belastungen durch die Konfrontation mit Gewaltdarstellungen, gewaltverherrlichenden oder anderweitig verstörenden Inhalten. Die Exposition gegenüber derartigen Inhalten sollte abhängig von der Resilienz der:des Mitarbeitenden begrenzt werden. Zudem sollte Mitarbeitenden eine Supervision angeboten werden.

2.3 Verantwortung gegenüber der Gesellschaft

Die Dimension gesellschaftlicher Verantwortung bezieht sich einerseits auf die gesellschaftliche Verantwortung von sozialwissenschaftlicher Forschung, einen Beitrag zur rationalen Lösung gesellschaftlicher Probleme zu leisten, anderseits auf die Verantwortbarkeit von möglichen, auch unintendierten Folgen für die Gesellschaft insgesamt.

In Hinblick auf den gesellschaftlichen Umgang mit Radikalisierungsphänomenen kommt der Radikalisierungsforschung kommt die Verantwortung zu, die theoretischen und empirischen Grundlagen für eine reflektierte gesellschaftliche Auseinandersetzung mit dem Radikalisierungsgeschehen sowie für eine effektive, reflexive und an demokratischen Grundwerten orientierte Präventionsarbeit und sicherheitsbehördliche Praxis zu leisten. So würde ein Absehen von der Beforschung der bezeichneten Phänomene bedeuten, Expertise zu Fragen des gesellschaftlichen Umfangs mit potentiell sicherheitsgefährdender Radikalisierung in digitalen Räumen einer Deutungshoheit der Sicherheitsbehörden zu überlassen. Zugleich ist es Verantwortung der Forschung, mögliche negative Folgen der eigenen Forschungstätigkeit für den gesellschaftlichen Zusammenhalt und Frieden zu antizipieren und entsprechende Risiken zu kontrollieren. Gerade anwendungsbezogene resp. praxisnahe Radikalisierungsforschung muss sich mit möglicherweise unintendierten gesellschaftlichen Effekten der eigenen Forschung befassen. Hierzu muss sie sich die Frage stellen wie die erarbeiteten Forschungsergebnisse in der Präventionsarbeit, in der Justiz, in Sicherheitsbehörden, in der Politik und insb. auch in den Medien verwendet bzw. rezipiert werden könnten. Dabei ist neben der von Forschenden intendierten Verwertung auch zu berücksichtigen, dass Praxisakteur:innen Forschungsergebnisse auch für von Forschenden nicht intendierte Zwecke verwenden könnten. Auf dieser Grundlage gilt es mögliche negative gesellschaftliche Folgen der Ergebnisverwertung zu antizipieren und die Eintrittswahrscheinlichkeit der jeweiligen Folgen abzuschätzen. Beispielsweise sollen im Verbundprojekt RadiGaMe Tools entwickelt werden, die Polizeibehörden bei der Auswertung von Daten aus Gaming-Plattformen und Messenger-Diensten unterstützen. Ein gesellschaftliches Risiko hierbei ist, dass entsprechende Tools für eine „rechtsstaatlich umstrittene Präventionspolitik“ (Birsl/Junk 2022, 67) genutzt werden. Um diesbezügliche Risiken der eigenen Forschung besser abzuschätzen zu können, gilt es, sich mit derzeitigen Praktiken und den technologischen Möglichkeiten polizeilicher Internetauswertungen zu beschäftigen.

Den jeweiligen Implikationen der eigenen gesellschaftlichen Verantwortung als Forschende sollte immer im Kontext des jeweils eigenen Forschungsvorhabens bzw. -gegenstandes ausführlich entweder im Rahmen einer geeigneten Ethik-Kommission oder eines

vergleichbaren Peer-Review Mechanismus innerhalb oder außerhalb der eigenen Institution Rechnung getragen werden. In der Praxis ließe sich dies etwa innerhalb von größeren Forschungsverbünden im Rahmen von Workshops oder mithilfe eines regelmäßig hinzugezogenen Ethik-Beirates umsetzen.

3. Leitlinien für eine ethisch kontrollierte Forschungspraxis

Die im Folgenden dargestellten Überlegungen sollen für die Forschungspraxis eine handhabbare Lösung für eine ethische kontrollierte Beforschung zugangsregulierter Online-Räume darstellen und haben damit nicht den Anspruch, vollumfänglich oder abschließend zu sein. Im ersten Teil werden allgemeine Anforderungen an Forschungsvorhaben, die sich verdeckt Zugang zu geschlossenen Gruppen verschaffen wollen, formuliert. Um Daten aus geschlossenen Online-Gruppen ethisch vertretbar zu erheben, muss das gesellschaftliche Interesse an der Forschung die schutzwürdigen Interessen der Beforschten erheblich überwiegen. Hierzu ist für jeden Online-Kommunikationsraum, aus dem Daten verdeckt erhoben werden sollen eine entsprechende Interessensabwägung, die den Besonderheiten des jeweiligen Raumes Rechnung trägt, vorzunehmen. Im zweiten Teil wird hierzu ein Verfahren vorgeschlagen.

3.1 Allgemeine Anforderungen

Die allgemeinen Anforderungen entsprechen im Wesentlichen guter wissenschaftlicher Praxis. Ebenso wie bei guter wissenschaftlicher Praxis lässt sich die Einhaltung und Umsetzung dabei sowohl als Teil des eigenen Forschungsprozesses als auch der Kontrolle durch die entsprechende wissenschaftliche Community begreifen. Für Vorhaben, die eine verdeckte Datenerhebung planen sind folgende Punkte besonders wichtig:

Wissenschaftlicher Erkenntnisgewinn: Der wissenschaftliche Zweck, zu dem Daten aus geschlossenen Online-Gruppen erhoben werden soll, muss nachvollziehbar dargelegt werden. Der angestrebte wissenschaftliche Erkenntnisgewinn sollte deutlich über den Stand der Forschung hinausgehen.

Gesellschaftlicher Nutzen und Wissenstransfer: Es muss dargelegt werden, welchen direkten oder indirekten Nutzen die erwarteten wissenschaftlichen Erkenntnisse für die gesellschaftliche Praxis (z.B. für Akteur:innen aus Zivilgesellschaft, Prävention, Politik, Polizei, Justiz) haben sowie welche Aktivitäten unternommen werden sollen, um die Erkenntnisse in die Praxis zu transferieren.

Geeignetheit und Erforderlichkeit verdeckter Datenerhebung: Ausführlich zu begründen ist die methodische Geeignetheit und Erforderlichkeit von Datenerhebungen in zugangsregulierten Gruppen zur Gewinnung der angestrebten Erkenntnisse. Es ist v.a. darzulegen, inwiefern alternative Methoden der Datenerhebung (z.B. Expert:innenwissen, Ermittlungsakten) nicht zur Verfügung stehen oder keinen hinreichenden Aufschluss geben können.

Forschungsfolgenabschätzung: Abzuschätzen sind die Folgen der Forschung für die beforschten Individuen, deren Daten erhoben, gespeichert und verarbeitet wurden, für das Untersuchungsfeld sowie für die Gesellschaft als Ganze. Dabei gilt es zunächst mögliche Risiken aufzuzählen und anschließend zu bewerten und zu begründen, wie hoch das Risiko ist. Schließlich sind Maßnahmen zur Risikominimierung aufzuzeigen. Die Forschungsfolgenabschätzung sollte auf begründeten Annahmen beruhen, die in einem entsprechenden Dokument zu explizieren sind. Durch die Forschungsfolgenabschätzung wird auch die Anforderung einer Datenschutzfolgeabschätzung erfüllt. Die Folgeabschätzung ist aber umfassender, da auch Folgen für nicht von Datenerhebungen unmittelbar Betroffene beleuchtet werden.

Datenschutz: Die aus geschlossenen Gruppen erhobenen personenbezogenen Daten sind hochsensibel, da sie aus vertraulicher Kommunikation stammen und die Betroffenen im Falle eines unberechtigten Zugriffs Dritter Schaden nehmen könnten. Es ist daher ein Datenschutzkonzept zu erstellen und mit dem behördlichen Datenschutzbeauftragten abzustimmen. In diesem müssen die Risiken für die Betroffenen abgeschätzt und entsprechend adäquate Vorkehrungen zum Schutz vertraulicher Daten dargelegt werden. Hierzu gehören die umgehende Pseudonymisierung der Daten sowie die Speicherung auf zugangsgesicherten, insbesondere durch Angriffe aus dem Internet geschützten Datenträgern. In dem Datenschutzkonzept gilt es zudem das Verfahren zur Abwägung zwischen den berechtigten Interessen der Beforschten und dem öffentlichen Gegenstandsinteresse darzulegen.

Schutzkonzept für die Forschenden: Auf Grundlage einer Risikoanalyse gilt es ein Konzept zum Schutz der Forschenden gegenüber möglichen Anfeindungen von Seiten des Untersuchungsfeldes zu erarbeiten. Es gilt die faktische Anonymität der Forschenden und ihrer Institution gegenüber dem verdeckt beforschten Untersuchungsfeld durch geeignete technische Maßnahmen sicherzustellen. Hierzu gehören die Nutzung eines VPN, die sorgsame Konzeption und Erstellung einer Online-Legendierung, die Kontrolle und Reflektion aller legendierten Interaktionen mit dem Untersuchungsfeld im Forschungsteam sowie eine risikoadäquat kontrollierte Außendarstellung des Forschungsprojektes.

Festlegung von Kriterien für meldewürdige Prüffälle: Vor Beginn der Feldphase sollte eine Schwelle für potenziell meldewürdige strafrechtlich oder gefahrenrechtlich relevante Inhalte festgelegt und begründet werden (siehe hierzu Kap. 2.1). Hinsichtlich der Prüffälle ist, sofern keine gesetzliche Anzeigepflicht besteht, eine Abwägung zwischen den durch (potenzielle) Straftaten betroffenen Schutzgütern und den im Falle einer Meldung bestehenden Beeinträchtigungen der Erreichung der Forschungsziele vorzunehmen. Mögliche Anhaltspunkte für eine solche Abwägung bei nicht anzeigepflichtigen Vorfällen liefern bspw. die Konzepte des warning behaviours (siehe etwa Allwinn/Böckler 2021, Melroy 2018, Melroy et al. 2019).

Belastungskontrolle und Supervision: Die Exposition von Mitarbeitenden gegenüber verstörenden Inhalten wie z.B. Gewalt- oder NS-Verherrlichung, muss abhängig vom individuellen Resilienz-Level begrenzt werden. Mitarbeitenden muss zudem eine Supervision angeboten werden.

Peer-Review: Die ethische Legitimität des geplanten methodischen Vorgehens muss in einem der ursprünglichen Institution externen peer review von anderen Fachwissenschaftler:innen mit ethischer und rechtlicher Expertise, vorzugsweise durch eine Ethik-Kommission, überprüft und bestätigt werden.

3.2 Verfahren zur Einzelfallprüfung

Für jeden zugangsregulierten Online-Raum, aus dem Daten erhoben werden sollen, gilt es die Erhebungsschwelle unter ethischen Gesichtspunkten zu prüfen. Im Mittelpunkt steht dabei eine Interessensabwägung zwischen den schutzwürdigen Belangen der Beforschten und dem öffentlichen Gegenstandsinteresse. Vorab ist zudem zu prüfen, a) ob ein verdeckter Zugang ohne Sicherheitsrisiken für die Forschenden möglich ist und b) ob die verdeckte Datenerhebung zur Erfüllung der Forschungsziele geeignet und erforderlich ist.

Vorprüfungen

a. Prüfung der Zugangshürde hinsichtlich des Schutzes der Forschenden

Im ersten Schritt ist zu prüfen, wie sich der Zugangsprozess zu dem fraglichen Online-Raum gestaltet und ob es möglich ist, die Zugangsvoraussetzungen unter Wahrung der

Anonymität der:des Forschenden zu erfüllen. Sofern eine direkte Interaktion mit Gruppenadministrator:innen in Form von Nachrichten, Chats oder auch Calls vorgesehen ist, gilt es sorgsam zu prüfen, ob die entwickelte Legendierung ausreichend ist oder ggf. fundiert werden müsste.

b. Prüfung der Eignung und Erforderlichkeit

Bei Datenerhebungen aus zugangsregulierten Räumen ist dem Prinzip der Datensparsamkeit große Beachtung zu schenken. Eignung und Erforderlichkeit bilden eine notwendige forschungsethische Bedingung einer Erhebung von Daten aus zugangsregulierten Gruppen ohne Wissen der Beteiligten. *Eignung* bezieht sich hier auf die Frage, ob die Kommunikationsdaten aus der beizutretenden Gruppe Aufschluss über den Gegenstand erwarten lassen. Hinweise darauf lassen sich aus dem Gruppennamen bzw. der Gruppenbeschreibung, aus Informationen über in den Gruppen aktive bereits bekannte Nutzer:innen oder einer Verlinkung beziehungsweise Bewerbung der Gruppe in anderen Gruppen, die von den Forschenden bereits gesichtet wurden, ableiten. Darüber hinaus kann im Sinne einer ersten kursorischen Sichtung der letzten Nachrichten oder anderer geteilter Inhalte innerhalb des Raumes eine zusätzliche Einschätzung erfolgen. *Erforderlichkeit* bezieht sich auf die Frage, ob die Erhebung weiterer personenbezogener Daten notwendig ist, um eine Datenbasis für die empirische Untersuchung zu erstellen, die die Qualitätskriterien der zum Einsatz kommenden Methoden der Datenerhebung erfüllen. Hierzu bedarf es eines Samplingplans, der dem Prinzip der Datensparsamkeit im hohen Maße Rechnung trägt.

Um die Eignung und Erforderlichkeit von Daten aus einer beizutretenden Gruppe prüfen zu können, müssen Forschende die Kommunikationsinhalte sichten und sich hierzu verdeckt Zutritt zur Gruppe verschaffen. Bereits die bloße Kenntnisnahme der Kommunikationsinhalte stellt eine Verletzung der Privatsphäre der Teilnehmenden dar. Es müssen daher vor dem Zutritt anhand vorliegender Informationen konkrete Anhaltspunkte vorliegen, dass die Kommunikationsinhalte für die Untersuchung des interessierenden Phänomens geeignet und erforderlich sein könnten. Fällt die Vorprüfung positiv aus, kann der Gruppe beigetreten werden. Sodann gilt es Eignung und Erforderlichkeit anhand der gesichteten Kommunikationsdaten eingehender zu prüfen.

Interessensabwägung

Im Rahmen der Interessensabwägung gilt es, das öffentliche Interesse an dem Forschungsgegenstand den im besonderen Einzelfall, d.h. hinsichtlich des zu beforschenden Online-Raums, bestehenden schutzwürdigen Interessen der Beforschten gegenüberzustellen. Die schutzwürdigen Interessen sind also für jeden zu beforschenden zugangsregulierten Online-Raum zu bewerten. Das öffentliche Gegenstandsinteresse kann dagegen nur im Ganzen, nicht jedoch hinsichtlich einer konkreten Datenquelle bewertet werden. Welche Daten zur Erfüllung des öffentlichen Gegenstandsinteresses, d.h. zur Erreichung der wissenschaftlichen Erkenntnisziele geeignet und erforderlich sind, muss nach rein wissenschaftlich-methodischen Maßstäben, d.h. unabhängig von der gesellschaftlichen Wahrnehmung und Bewertung der jeweiligen Datenquelle, begründen werden.

Eine verdeckte Datenerhebung kann ethisch nur dann gerechtfertigt werden, wenn das öffentliche Gegenstandsinteresse das schutzwürdige Interesse der Beforschten erheblich überwiegt. Zur Gegenüberstellung von beiden Interessen wird vorgeschlagen, die Gewichtigkeit der Interessen jeweils auf einer vierstufigen Likert-Skala (niedrig, mittel, hoch, sehr hoch) einzuschätzen, wobei eine Stufengleichheit ein nicht-überwiegendes Interesse indiziert, während ein Stufenunterschied als erheblich überwiegendes Interesse gewertet werden kann.

I. Gesellschaftliches Interesse

Die Gesellschaft fragt Reflexions -und Problemlösungswissen hinsichtlich des gesellschaftlichen Umgangs mit demokratie- und sicherheitsgefährdenden Phänomenen nach. Die Herausforderung besteht nun darin, das Ausmaß des Gegenstandsinteresses strukturiert und nachvollziehbar einzuschätzen und zu begründen. Hierzu werden zwei Kriterien vorgeschlagen:

Ia. Bedrohung für das demokratische Gemeinwesen

Das gesellschaftliche Interesse an Radikalisierungsforschung ist umso höher, je bedrohlicher Radikalisierungsphänome von der Gesellschaft wahrgenommen werden. Dabei geht es insbesondere um die wahrgenommene Bedrohung für das gesellschaftliche Zusammenleben, für demokratische Institutionen sowie für die Sicherheit von Bürger:innen. Das gesellschaftliche Interesse an Radikalisierungsforschung korreliert mit der wahrgenommenen Bedrohung durch Radikalisierungsphänomene, wobei diese Wahrnehmung nicht immer der realen Gefährdungslage entspricht. Öffentliche Sicherheitsdiskurse prägen maßgeblich die gesellschaftliche Bedrohungswahrnehmung, indem sie bestimmte Gefahren identifizieren und hervorheben, während andere möglicherweise unterschätzt werden (vgl. Krasmann et al. 2014). So kann beispielsweise die Bedrohung durch rechtsextreme Akteur:innen in der öffentlichen Wahrnehmung in den Hintergrund treten, obwohl sie objektiv betrachtet eine erhebliche Gefahr darstellt. Vor diesem Hintergrund sollte für den Zweck der hier gegenständlichen Interessensabwägung die Bedrohlichkeit eines Radikalisierungsgeschehens an möglichst objektiven Kriterien eingeschätzt werden. Gegenstand der Einschätzung sollten dabei die konkret zu beforschenden Gruppierungen, Szenen oder Bewegungen sein, nicht jedoch der Phänomenbereich als Ganzer (etwa der „Rechtsextremismus“). Vorgeschlagen werden folgende Kriterien zur Einschätzung der Bedrohlichkeit, die für den jeweiligen Forschungsgegenstand zu spezifizieren wären: 1. die Demokratie- und Menschenfeindlichkeit der Ideologie und Zielsetzungen der untersuchten Akteur:innen, 2. der Radikalisierungsgrad, insb. in Hinblick auf Gewalt und 3. das Mobilisierungspotential der Akteur:innen.

Ib. Akteursübergreifend artikulierte Problemlösungsbedarfe

Ferner kann ein umso höheres gesellschaftliches Interesse am Gegenstand der Forschung angenommen werden, je umfassender und dringlicher sich die Problemlösungsbedarfe aus Sicht der Praxis stellen. Um zu einer entsprechenden Einschätzung zu gelangen, sind Forschende angehalten, sich differenziert mit den Praxisfeldern der Bearbeitung des Radikalisierungsgeschehens zu befassen, um zu verstehen, wie der Stand der Praxis ist und wo Wissens- und Maßnahmenlücken gesehen werden. Dabei sollten die Problemlösungsbedarfe über die verschiedenen Sektoren gesellschaftlicher Praxis (z.B. Sicherheitspraxis, Prävention, Zivilgesellschaft) hinweg erfasst werden. Sofern dafür nicht auf vorhandene Literatur zurückgegriffen werden kann, sollte im Rahmen des Forschungsvorhabens mindestens eine explorative Praxisfeldanalyse gestützte auf Expert:inneninterviews durchgeführt werden. Vorgeschlagen wird, beide Bewertungsdimensionen des gesellschaftlichen Gegenstandsinteresses (Ia, Ib) jeweils auf einer vierstufigen Likert-Skala (niedrig, mittel, hoch, sehr hoch) einzuschätzen und den Mittelwert für die Gesamteinschätzung heranzuziehen.

II. Schutzwürdige Interessen der Beforschten

Für die Bewertung der schutzwürdigen Interessen der Beforschten hinsichtlich konkreter Online-Räume wird ein standardisiertes Verfahren vorgeschlagen, um die Praktikabilität, Nachvollziehbarkeit und methodische Kontrolle der Einschätzung der schutzwürdigen Interessen in der Forschungspraxis im Falle einer Vielzahl zu bewertender Räume zu erhöhen. Vorgeschlagen werden hierzu folgende drei Kriterien. Um zu einer strukturierten und

nachvollziehbaren Gesamteinschätzung des Schutzwürdigkeitsinteresses zu gelangen, wird vorgeschlagen, alle drei Kriterien auf einer vierstufigen Likert-Skala (niedrig, mittel, hoch, sehr hoch) einzuschätzen und die mittlere Ausprägung als Grundlage für die Gesamteinschätzung heranzuziehen.

IIa. Privatheitsbezug der geteilten Inhalte

In dieser Kategorie gilt es den Privatsphärebezug der im jeweiligen Kommunikationsraum geteilten Inhalte zu bewerten. Wie in Kap. 2.1 erläutert, muss davon ausgegangen werden, dass auch rein politische Diskussionen in zugangsregulierten Räumen, die Aufschluss über individuelle politische Haltungen geben, aber keine Bezüge zum (sonstigen) Privatleben der Akteur:innen erkennen lassen, als Teil der Privatsphäre zu betrachten sind. Es gilt daher zu bewerten, in welchem Ausmaß die geteilten Informationen Einblick in die Privatsphäre der Nutzenden ermöglichen. Dazu gehören etwa die individuelle Gesinnung, politische und soziale Aktivitäten, die Persönlichkeit und die persönlichen Lebensumstände.

Tab. 1: Privatheitsbezug der geteilten Inhalte

Niedrig	Weltanschauliche und politische Themen werden weitestgehend ohne Bezug zu Fragen der individuellen Alltagsgestaltung und politischen Praxis bearbeitet. Die Daten geben lediglich über individuelle Haltungen und Einstellungen Aufschluss.
Mittel	Über Haltungen zu weltanschaulichen und politischen Themen hinaus werden in einem begrenzten Rahmen Informationen über die individuelle Alltagspraxis offenbart (z.B. Alltagserlebnisse, Berufstätigkeit, politische Aktivitäten). Im Zentrum stehen jedoch weltanschauliche und politische Themen. Dadurch lassen sich soziale und persönlichkeitsbezogene Profil erstellen.
Hoch	Offenlegung erweiterter Informationen zum Privaterleben: Nutzer:innen teilen regelmäßig erweiterte Informationen zu ihrem Privatleben, z.B. Hobbys, Beziehungen, psychologische Selbstreflexionen, persönliche Lebensumstände, aus denen sich umfassendere soziale und persönlichkeitsbezogene Profile ableiten lassen.
Sehr hoch	Offenlegung von Informationen aus der Intimsphäre: Nutzer:innen teilen regelmäßig Informationen aus der Intimsphäre.

IIb. Privatheitserwartungen im Kontext der Gruppengröße

Innerhalb dieser Kategorie wird die jeweilige Zugangsbarriere des zugangsregulierten digitalen Raums anhand eines Stufensystems (vgl. Kap. 2.1) beurteilt. Verbunden mit der Zugangsbarriere sind Erwartungen der Teilnehmenden an den geschützten Kommunikationsraum. Je höher die Barriere, desto „sicherer" erscheint der jeweilige Kommunikationsraum in der Eigenwahrnehmung.

Tab. 2: Privatheitserwartungen

Niedrig	Geringe Privatheitserwartungen: Empfänger:innenkreis wird nur sehr vage begrenzt, da keine Prüfung der Gesinnung/Interessen stattfindet; Zugang durch Beantwortung einer Frage möglich.
Mittel	Mittlere Privatheitserwartungen: Empfänger:innenkreis wird nach festgelegten Kriterien begrenzt, die standardisiert überprüft werden; Teilnehmende erfüllen Kriterien unzuverlässig, da Täuschung mit mittlerem Aufwand möglich ist. Die beschriebene Zugangsbarriere könnte bei kleineren Gruppen (< 15 Teilnehmende) auch hohe Privatheitserwartungen induzieren.
Hoch	Hohe Privatheitserwartungen: Empfänger:innenkreis wird nach festgelegten Kriterien begrenzt, die eingehend individuell überprüft werden; Täuschung erfordert höheren Aufwand.

	Die beschriebene Zugangsbarriere könnte bei kleineren Gruppen (< 15 Teilnehmende) auch sehr hohe Privatheitserwartungen induzieren. Bei sehr großen Gruppen (> 100 Teilnehmende) könnten dagegen auch mittlere Privatheitserwartungen angenommen werden.
Sehr hoch	Sehr hohe Privatheitserwartungen: Umfassende individuelle Prüfung inkludiert Offenlegung der personalen Identität oder persönlicher Bekanntschaft des:der Anfragenden

IIc. Teilnahme von Minderjährigen

Eine besondere Schutzbedürftigkeit besteht bei minderjährigen Personen. Es handelt sich bei Minderjährigen um eine besonders vulnerable Gruppe von Nutzer:innen, weil diese sich der Risiken und Folgen ihrer Online-Aktivitäten für den Schutz ihrer Persönlichkeitsrechte möglicherweise weniger bewusst ist (Rau et al. 2021: 7). Für die Einschätzung der schutzwürdigen Interessen der Betroffenen in den zu beforschenden geschlossenen Räumen ist daher von entscheidender Bedeutung, ob es Anzeichen innerhalb der jeweiligen digitalen Räume gibt, dass Minderjährige unter den Teilnehmenden sind. Dabei soll eine Beforschung von minderjährigen Nutzer:innen ohne informierte Einwilligung nicht grundsätzlich ausgeschlossen werden. Vielmehr geht es darum, die besondere Schutzbedürftigkeit von Minderjährigen in der Gesamtbewertung der schutzwürdigen Interessen der in den zu beforschenden Räumen interagierenden Nutzer:innen angemessen zu berücksichtigen.

Laut Nutzungsbedingungen sind viele der Plattformen, die im Rahmen des Forschungsvorhabens untersucht werden, ab einem Mindestalter von 16 Jahren, wie zum Beispiel Telegram und Discord. Ausnahmen bilden hier Plattformen wie YouTube und Steam, die bereits ab 13 Jahren zugelassen sind. Jedoch ist in vielen Fällen davon auszugehen, dass das entsprechende Alter einiger Nutzer:innen deutlich niedriger liegen dürfte. Aus forschungsökonomischen Gründen kann jedoch auch hier, ähnlich wie bei der Einwilligung, angeführt werden, dass die Überprüfung jedes einzelnen Teilnehmenden nicht praktikabel wäre. Deshalb können Maßnahmen zur Exkludierung minderjähriger Teilnehmender aus der Datenerhebung, mit dem Ziel, das Ausmaß des Eingriffs in schutzwürdige Interessen von Betroffenen zu reduzieren, nur in Fällen, in denen es Anzeichen für die Minderjährigkeit der jeweiligen Teilnehmenden gibt, getroffen werden.

Im Zusammenhang mit Radikalisierung auf Gaming-Plattformen sind in den letzten Jahren vorwiegend von Minderjährigen genutzte Plattformen in den Fokus der Aufmerksamkeit gerückt. Der primäre Nutzungszweck dieser Plattformen ist zwar weiterhin das Spielen digitaler Spiele, einige von ihnen sind insbesondere bei jungen Menschen zu sozialen Medien geworden. Da davon auszugehen ist, dass hier vorrangig Minderjährige kommunizieren, besteht in diesem Fall eine sehr hohe Schutzbedürftigkeit der zu beforschenden Kommunikation (siehe Tab. 3), gleichzeitig aufgrund der potenziellen Vulnerabilität der Zielgrupe, aber auch eine hohes Forschungsinteresse seitens der RadikalisierungsforschungEntsprechend stellt sich die Hürde für eine Datenerhebung aus geschlossenen Räumen, insb. bei einer hohen Zugangsbarriere (siehe IIb), auf dieser Plattform als sehr hoch dar.

Tab. 3: Besondere Schutzbedürftigkeit durch Teilnahme von Minderjährigen

Niedrig	Keine Hinweise auf Präsenz von Minderjährigen
Mittel	Es liegen Hinweise auf die Präsenz einzelner Minderjähriger vor, die von der Datenerhebung ausgeschlossen werden können.
Hoch	Es liegen Hinweise auf die Präsenz einer größeren Zahl von Minderjährigen vor, die sich nicht sicher bestimmen lassen. Es besteht hohes Risiko, dass nicht alle Minderjährige von der Datenerhebung ausgeschlossen werden können.

Sehr hoch	Es liegen Hinweise vor, dass in der Online-Gruppe vorrangig Minderjährige kommunizieren.

Die ausgeführten Überlegungen sollen im Folgenden kurz anhand eines fiktiven Beispiels im Bereich des militanten Akzelerationismus auf der Plattform Telegram skizziert werden. Die folgenden Ausführungen sollen an dieser Stelle lediglich exemplarisch für die oben aufgeworfenen Überlegungen stehen und spiegeln nicht vollumfänglich die angestrebten Reflektionen, die im Rahmen eines Forschungsprojektes durchzuführen sind.

Angenommen im Rahmen der allgemeinen Feldexploration wurden bereits einige Kanäle identifiziert, die für das Forschungsvorhaben von Relevanz sind. Bei Kanälen auf Telegram handelt es sich um öffentlich zugängliche Daten, in Form der sogenannten „one to many" Kommunikation. Über diese Kanäle könnten im angenommenen Beispiel durch geteilte Links einige Gruppen identifiziert werden, von denen angenommen werden kann, dass sie für das Forschungsvorhaben ebenso von Interesse wären. Da es sich hierbei im Zweifelsfall um zugangsregulierte Kommunikationsräume handelt, muss eine Einzelfallprüfung vorgenommen werden. Die fiktive Beispielgruppe soll hier der Veranschaulichung nach „1488 Memekämpfer" heißen.

Im Rahmen des oben beschriebenen Vorgehens müssten im ersten Schritt Vorprüfungen vorgenommen werden, zunächst was die angenommene Zugangshürde betrifft und anschließend die Eignung und Erforderlichkeit. Sofern im Zusammenhang mit einem gepostеten Link zu einer Gruppe keine weitere Information gepostet wurde, die auf eine erhöhte Zugangshürde rückschließen lässt, könnte zunächst getestet werden, ob die entsprechende Gruppe frei einsehbar ist, ohne, dass ein Beitritt erforderlich ist. In einem solchen Fall kann angenommen werden, dass die Zugangsvoraussetzungen eher niedrig sind. In Einzelfällen kann dies jedoch auch nicht der Fall sein. Muss ein Beitritt dagegen erst angefragt und durch einen Administrator bestätigt werden, kann davon ausgegangen werden, dass es eventuell zu weiteren Prüfungsschritten seitens der Administrator:innen kommt. Hier gilt es, die eigene Legendierung zu reflektieren, eine Abbruchoption bereit zu haben oder von einem Beitritt gänzlich abzusehen.

Im Zuge dieser ersten Überprüfung lässt sich in der Regel bereits eine erste Einschätzung hinsichtlich der Eignung der Kommunikationsdaten aus der Gruppe vornehmen. In Bezug auf die Erforderlichkeit wäre hier zu reflektieren, wie welche anderen Daten im Rahmen des Forschungsvorhabens bereits erhoben wurden und inwiefern die eventuelle Erhebung der entsprechenden Gruppe die eigene Datenbasis erweitert. Fällt diese erste Vorprüfung positiv aus, kann im Rahmen einer ersten Sichtung des Kommunikationsgeschehens nochmals intensiver mit Blick auf Eignung und Erforderlichkeit weiter exploriert werden.

> Für das Beispiel der Gruppe „1488 Memekämpfer" wird festgestellt, dass die entsprechende Gruppe frei einsehbar ist. Der erste Blick in den Chatverlauf lässt durch bereits gepostete diskriminierende und menschenverachtende Memes eine Relevanz für das Forschungsvorhaben feststellen. Durch das kurze Sichten der letzten 30 Nachrichten fällt auf, dass neue Mitglieder des Kommunikationsraums kurz angesprochen werden und sich nach dem Auffinden des Links erkundigt wird. Es fällt allerdings auch auf, dass durch das hohe Kommunikationsaufkommen nur ein Teil der Nutzer:innen diese Nachrichten beantwortet. Für das weitere Vorgehen wird nochmals kurz die eigene Legende überprüft, sich für einen Beitritt entschieden und erst auf ein wiederholtes Nachfragen bzw. Angesprochen-Werden überhaupt zu reagieren. Der Beitritt wird durch einen Administrator genehmigt und obwohl die Nachfrage nicht beantwortet wird, erfolgt kein Bann

aus der Gruppe, da ein hohes Kommunikationsgeschehen innerhalb der Gruppe vorherrschend ist. Für das Beispiel soll davon ausgegangen werden, dass soweit noch keine Daten erhoben wurden und die Erforderlichkeit ebenso gegeben ist.

Der Kern der Einzelfallprüfung bildet nun die Interessensabwägung. Hierzu ist zunächst das öffentliche Gegenstandsinteresse einzustufen. Für die allgemeine Bewertung der gesellschaftlichen Bedrohung (siehe Ia) durch den Akzelerationismus wurde dafür

- *erstens* die Demokratie- und Menschenfeindlichkeit der Ideologie und Zielsetzungen der radikalisierten Akteur:innen als sehr hoch bewertet. Kern des akzelerationistischen Selbstverständnisses bilden nicht nur die Bezugnahme auf die Annahme eines „white genocide“, also der verschwörungsideologischen Annahme, dass das weiße Volk systematisch u.a. durch Bevölkerungsaustausch bekämpft wird, sondern darüber hinaus die Annahme, dass eine als weiß konstruierte „Rasse“ anderen Bevölkerungsgruppen überlegen sei. Darüber hinaus wird die Demokratie in ihrer jetzigen Form kategorisch abgelehnt und stattdessen die Etablierung eines faschistischen Staates angestrebt (Dittrich et al. 2022: 14f).

- *zweitens* der Radikalisierungsgrad, insb. in Hinblick auf Gewalt ebenso als sehr hoch eingestuft. Dies begründet sich durch die starke Affirmation und Verherrlichung von Gewalt als legitimen Mittel zur Durchsetzung des eigenen Interesses, welches insbesondere in der Vertiefung von Spaltungen innerhalb demokratischer Gesellschaften, mit dem Ziel, diese zum Zusammenbruch zu bringen, um eine faschistische Gesellschaftsordnung etablieren zu können, liegt. Nicht nur sind zahlreiche Anschläge bekannt, die einer akzelerationistischen Ideologie zugerechnet werden können, sondern darüber hinaus findet sich sowohl in den einschlägigen Online Publikationen als auch innerhalb des öffentlichen Kommunikationsgeschehens eine große Nähe zu exzessiven Gewaltdarstellungen.

- *drittens* das Mobilisierungspotential der untersuchten Akteur:innen als mittel eingestuft. Obwohl argumentiert werden kann, dass es sich beim militanten Akzelerationismus nach wie vor um ein Randphänomen innerhalb der extremen Rechten handelt, kann angenommen werden, dass trotzdem durch die ideologische Ausrichtung an nationalsozialistischen Ideologieelementen ein hohes Anschlusspotential an andere Teile der extremen Rechten besteht. Darüber hinaus kann ein hohes Mobilisierungspotential einerseits durch die zahlreichen Fälle von Strafverfahren innerhalb Deutschlands, wie z.B. der „Atomwaffendivision Deutschland“ oder auch der „Totenwaffen Division“ begründet werden. Ausdruck eines potentiell hohen Mobilisierungspotentials ist andererseits das häufig niedrige Alter der jeweils Verdächtigen. So war ein 2023 in Verbindung mit der Feuerkrieg Division Verhafteter lediglich 13 Jahre alt. Ein sehr hohes Mobilisierungspotential kann nicht angenommen werden, da der Akzelerationismus über keine Resonanzbasis in der breiteren Bevölkerung verfügt.

Auch die Bewertung der akteursübergreifend artikulierten Problemlösungsbedarfe führt zu einer sehr hohen Einstufung. Zuallererst können dabei die verschiedenen Aufforderungen zivilgesellschaftlich organisierter Betroffener rechter Gewalt, wie z.B. die gemeinsame Pressemitteilung zur Urteilsverkündung im Halle-Prozess des VBRG (VBRG 2020), herangezogen werden, die eine effizientere Bekämpfung extrem rechter Gewalttaten fordern. Außerdem stellen Sicherheitsbehörden wie das Bundesamt für Verfassungsschutz eine Ge-

fahr durch rechtsterrorisiische Anschläge fest und heben die besondere Bedeutung der Beobachtung des gewaltorientierten Rechtsextremismus hervor (BMI 2024: 80). Das Gegenstandsinteresse kann somit zusammenfassend als sehr hoch eingestuft werden.

Den bisher erfolgten Überlegungen zum öffentlichen Gegenstandsinteresse sollen im Folgenden Überlegungen zu den schutzwürdigen Interessen der Beforschten anhand des fiktiven Beispiels der „1488 Memekämpfer“ gegenübergestellt werden:

- *erstens* hinsichtlich des Privatheitsbezugs der geteilten Inhalte (siehe IIa). In einer ersten groben Sichtung der geteilten Kommunikationsinhalte werden in einem ersten Schritt die letzten 50 Nachrichten der Gruppe gelesen. Es bestätigt sich die Annahme, dass es sich vornehmlich um geteilte und weitergeleitete Inhalte der Nutzenden aus anderen digitalen Räumen auf Telegram und Tiktok handelt. Es werden viele diskriminierende Sticker als Reaktionen auf die Inhalte geteilt. Darunter fallen z.B. Abbildungen von Breivik, während er den Hitlergruß zeigt, Pepe der Frosch in SS-Uniform oder die Abbildung einer Person, die der LGBTIQ+ Community zugehörig sein soll, die sich gerade erhängt. Es fallen keine Bezüge zur Privat- oder Intimsphäre der Teilnehmenden auf. In einem zweiten Schritt werden die geteilten Bilder der Gruppe aufgerufen, um hier ebenso eine erste Sichtung vorzunehmen. Bei der Durchsicht der letzten Monate fallen lediglich vereinzelt durch die Teilnehmenden verpixelte Selfies oder Bilder auf, in welchen sie ihre Gewaltbereitschaft via Equipment versuchen zu demonstrieren. In einem dritten Schritt wird die schriftliche Kommunikation anhand von 50 Nachrichten aus zwei weiteren Stichproben jeweils zu vier und zwölf Wochen zurückliegenden Zeitpunkten überprüft. Bei dieser Überprüfung fallen ebenso keine Bezüge zur Privat- oder Intimsphäre der Teilnehmenden auf. Der Privatheitsbezug aufgrund der Kommunikationsinhalte wird daher auf mittel eingestuft, da durch die beschriebenen Selfies zwar ein minimaler Einblick in die individuelle Alltagspraxis der Poster:innen möglich ist, jedoch darüber hinaus keine weiteren Bezüge erkennbar werden.

- *zweitens* werden die Privatheitserwartungen (IIb) als niedrig eingeschätzt, da der Zugang zur Gruppe lediglich durch eine Nachfrage überprüft wird, jedoch eine Teilnahme auch bei Nichtbeantwortung möglich ist. Des Weiteren verfügt die Gruppe über eine hohe dreistellige Anzahl von Nutzenden, sodass angenommen werden kann, dass allen Teilnehmenden die mögliche Größe des Empfänger:innenkreises bewusst ist.

- *drittens* wurden im Rahmen der explorativen Sichtung der Kommunikationsdaten keine Hinweise auf eine eventuelle Minderjährigkeit der Teilnehmenden im Gruppenchat gefunden. Daher wird die besondere Schutzbedürftigkeit durch Teilnahme von Minderjährigen als niedrig eingestuft. Sollte im Rahmen des Auswertungsprozesses der Daten dennoch die Minderjährigkeit einzelner Teilnehmenden nachträglich festgestellt werden, könnten diese innerhalb des Datensatzes kenntlich gemacht und ihre Nachrichten vom Auswertungsprozedere ausgeschlossen werden.

Im Vergleich zu dem als sehr hoch eingestuften öffentlichen Gegenstandsinteresse wurden die schutzwürdigen Interessen der Beforschten im hiesigen Beispiel der Gruppe „1488 Memekämpfer“ als niedrig eingestuft. Daher wäre im hier angeführten Beispiel eine Erhe-

bung durch den Stufenunterschied der Einstufung als forschungsethisch gerechtfertigt anzusehen, da eine weit überwiegendes öffentliches Gegenstandsinteresse angenommen werden kann.

Literatur

Allwinn, M./Böckler, N. (2021): Crawling in the dark—Perspectives on threat assessment in the virtual sphere, in: Meloy, J. R./Hoffmann, J. (Hg.): International handbook of threat assessment, Oxford University Press, Oxford, S. 283–300.

American Sociological Association (1999): Code of Ethics and Policies and Procedures of the ASA Committee on Professional Ethics, Washington, D.C.

Birsl, U./Junk, J. (2022): Wissenschaft und Verantwortung: Ethische Einordnungen sozialwissenschaftlicher Forschung in sozialen Medien, in: Birsl, U. et al. (Hg.): Inszenieren und Mobilisieren: Rechte und islamistische Akteure digital und analog, Bielefeld, S. 59-78.

Bulmer, M. (1980): Comment on 'The Ethics of Covert Methods', in: The British Journal of Sociology 31 (1), S. 59-65.

Bulmer, M. (1982): Ethical Problems in Social Research: the case of covert participant observation, in: Ders. (Hg.): Social Research Ethics: An Examination of the Merits of Covert Participant Observation, London, S. 3-12.

Bundesministerium des Innern und für Heimat (2024): Verfassungsschutzbericht 2023, Berlin.

Conway, M. (2021): Online Extremism and Terrorism Research Ethics: Researcher Safety, Informed Consent, and the Need for Tailored Guidelines, in: Terrorism and Political Violence 33 (2), S. 367-380.

Demant, J./Moretti, A. (2024): Intrusiveness and the Public-private Divide in Netnography: A Situated, Structured Approach for Ethical Research in the Context of Closed, Group-based, or Hidden Social Media Behaviour, in: International Journal of Qualitative Methods 23, S. 1-15.

Deutsche Gesellschaft für Soziologie (DGS)/Berufsverband Deutscher Soziologen (BDS) (2017): Ethik-Kodex der Deutschen Gesellschaft für Soziologie (DGS) und des Berufsverbandes Deutscher Soziologinnen und Soziologen (BDS), Essen/Frankfurt am Main.

Dittrich, M./Rathje, J./Manemann, T./Müller, F. (2022): Militanter Akzelerationismus: Ursprung und Aktivität in Deutschland, CeMAS Center für Monitoring, Analyse Strategie, Berlin.

Dodds, A. J. (2004): A Reply to Wells, in: Graduate Journal of Social Science 1 (1), S. 24-29.

Franzke, A. S./Bechmann, A./Zimmer, M./Ess, C. M./Association of Internet Researchers (2020): Internet Research: Ethical Guidelines 3.0, Association of Internet Researchers, Chicago.

Golla, S. J./Hofmann, H./Bäcker, M. (2019): Connecting the Dots. Sozialwissenschaftliche Forschung in sozialen Online-Medien im Lichte von DS-GVO und BDSG-neu, in: Aldenhoff, C. et al. (Hg.): Digitalität und Privatheit. Kulturelle, politisch-rechtliche und soziale Perspektiven, Bielefeld, S. 225–251.

Guhl, J./Ebner, J./Rau, J. (2020): Das Online-Ökosystem rechtsextremer Akteure, Institute for Strategic Dialogue, London.

Heise, N./Schmidt, J.-H. (2014): Ethik der Onlineforschung, in: Welker, M. et al. (Hg.): Handbuch Online-Forschung, Köln, S. 519-539.

Holdaway, S. (1982): An Inside Job: A Case Study of Covert Research on the Police, in: Bulmer, M. (Hg.): Social Research Ethics: An Examination of the Merits of Covert Participant Observation, London, S. 59-79.

Hopf, C. (2000): Forschungsethik und qualitative Forschung, in: Flick, U. et al. (Hg.): Qualitative Forschung. Ein Handbuch, Reinbek bei Hamburg, S. 589-599.

Krasmann, S./Kreissl, R./Kühne, S./Paul, B./Schlepper, C. (2014): Die gesellschaftliche Konstruktion von Sicherheit. Zur medialen Vermittlung und Wahrnehmung der Terrorismusbekämpfung, Forschungsforum Öffentliche Sicherheit, Berlin.

Lauder, M. A. (2003): Covert Participant Observations of a Deviant Community: Justifying the Use of Deception, in: Journal of Contemporary Religion 18 (2), S. 186-196.

Meloy, J. R. (2018): The operational development and empirical testing of the Terrorist Radicalization Assessment Protocol (TRAP–18), in: Journal of Personality Assessment 100 (5), S. 483-492.

Meloy, J. R./Goodwill, A. M./Meloy, M. J./Amat, G./Martinez, M./Morgan, M. (2019): Some TRAP-18 indicators discriminate between terrorist attackers and other subjects of national security concern, in: Journal of Threat Assessment and Management 6 (2), S. 93-110.

Poscher, R. (2010): Menschenwürde und Kernbereichsschutz. Von den Gefahren einer Verräumlichung des Grundrechtsdenkens, in: Humboldt Forum Recht 7, S. 90-103.

Rat für Sozial- und Wirtschaftsdaten (RatSWD) (2023): Handreichung „Umgang mit der Kenntnisnahme von Straftaten im Rahmen der Durchführung von Forschungsvorhaben", Berlin.

Rau, J./Münch, F./Asli, M. (2021): SOCRATES: Social Media Research Assessment Template for Ethical Scholarship, (Social) Media Observatory, Berlin.

Sold, M. (2022): Von Cyber-Da'wa bis zur Gewalt: Mobilisierungstechniken radikaler salafistischer Personen, in: Birsl, U. et al. (Hg.): Inszenieren und Mobilisieren: Rechte und islamistische Akteure digital und analog, Bielefeld, S. 181-214.

Sold, M./Junk, J. (2021): Untersuchung extremistischer Inhalte auf Social-Media-Plattformen: Datenschutz und Forschungsethik – Herausforderungen und Chancen, Global Network in Extremism & Technology, London.

Verband der Beratungsstellen für Betroffene rechter, rassistischer und antisemitischer Gewalt e.V. (VBRG) (2020): „Alle, die sich gegen Antisemitismus, Rassismus und Rechtsextremismus einsetzen, sollten den Nebenkläger*innen für ihren Mut und ihr gesellschaftliches Engagement dankbar sein.", Berlin.

Wells, H. M. (2004): Is there a place for covert research methods in criminology, in: Graduate Journal of Social Science 1 (1), S. 1-19.

Wolff, S. (2000): Wege ins Feld und ihre Varianten, in: Flick, U. et al. (Hg.): Qualitative Forschung. Ein Handbuch, Reinbek bei Hamburg, S. 334-349.