

### Navigating a Rugged Coastline - Ethics in empirical (De-)Radicalization Research

Eppert, Kerstin; Frischlich, Lena; Bögelein, Nicole; Jukschat, Nadine; Reddig, Melanie; Schmidt-Kleinert, Anja

Veröffentlichungsversion / Published Version

Sonstiges / other

#### Empfohlene Zitierung / Suggested Citation:

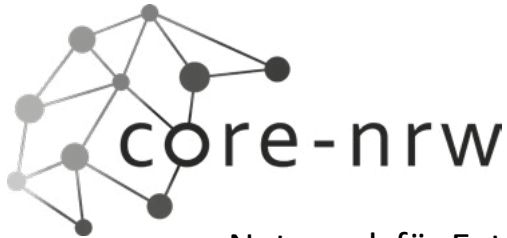
Eppert, K., Frischlich, L., Bögelein, N., Jukschat, N., Reddig, M., & Schmidt-Kleinert, A. (2020). *Navigating a Rugged Coastline - Ethics in empirical (De-)Radicalization Research*. Bonn: CoRE-NRW - Connecting Research on Extremism in North Rhine-Westphalia / Netzwerk für Extremismusforschung in Nordrhein-Westfalen. <https://nbn-resolving.org/urn:nbn:de:0168-ssoar-67918-5>

#### Nutzungsbedingungen:

Dieser Text wird unter einer CC BY Lizenz (Namensnennung) zur Verfügung gestellt. Nähere Auskünfte zu den CC-Lizenzen finden Sie hier: <https://creativecommons.org/licenses/by/4.0/deed.de>

#### Terms of use:

This document is made available under a CC BY Licence (Attribution). For more information see: <https://creativecommons.org/licenses/by/4.0>



Netzwerk für Extremismusforschung  
in Nordrhein-Westfalen

CoRE – Connecting Research  
on Extremism in  
North Rhine-Westphalia

# NAVIGATING A RUGGED COASTLINE

**Ethics in Empirical (De-)Radicalization Research**

Kerstin Eppert | Lena Frischlich | Nicole Bögelein  
Nadine Jukschat | Melanie Reddig | Anja Schmidt-Kleinert

**SUMMARY ZUSAMMENFASSUNG**

The current paper documents the results of a multi-disciplinary international workshop on ethics in (de-)radicalization research, organized by the authors at the Bochum Center for Advanced Internet Studies (CAIS) in March 2019.\* In light of the specificity of each research context, this paper aims to develop a baseline for ethical standards across projects, disciplines and contexts. The aim is to provide the instruments that allow for a project-specific setup that enables researchers to develop their own concepts and solutions in the context of their empirical field. The following sections elaborate on the above issues, pointing to practices and possible proceedings so as to ensure ethical standards in (de)radicalization research.

Das vorliegende Forschungspapier dokumentiert die Ergebnisse eines multidisziplinären internationalen Workshops zur Ethik in der (De-)Radikalisierungsforschung, den die Autorinnen im März 2019 am Bochumer Center for Advanced Internet Studies (CAIS) organisiert haben.\* Im Hinblick auf die Besonderheiten der einzelnen Forschungskontexte soll dieses Papier eine projekt-, disziplin- und kontextübergreifende Basis für ethische Standards entwickeln. Ziel ist es, Instrumente bereitzustellen, die eine projektspezifische Aufstellung ermöglichen, die Forscherinnen und Forscher befähigt, eigene Konzepte und Lösungen im Kontext ihres empirischen Feldes zu entwickeln. Die folgenden Kapitel gehen auf die oben genannten Fragen ein und weisen auf Praktiken und mögliche Vorgehensweisen hin, um ethische Standards in der (De-)Radikalisierungsforschung zu gewährleisten.

\* The work on “Ethics in (De)Radicalization Research” goes back to the work of an off-spring working group to the network Connecting Research on Extremism (CoRE) in North Rhine-Westphalia, CoRE Digital, that was constituted in 2017 and in which the authors are active. We are grateful for the synergetic effects of the network. Our deep gratitude further goes to the Bochum Center for Advanced Internet Studies (CAIS) who provided financial and organizational support to an interdisciplinary peer workshop that we consider the kick-off for what we hope to become a continuous dialogue in online and offline research.

**CONTENTS**

<b>1</b>	<b>Research ethics in (de-)radicalization research</b>	<b>3</b>
<b>2</b>	<b>Research context and project set-up</b>	<b>4</b>
2.1	Empirical (de-)radicalization research in context	4
2.2	Awareness and transparency regarding public and private obligations	5
2.3	Mapping the field and determining operational requirements	5
2.4	Setting up accountability mechanisms	6
<b>3</b>	<b>Data collection</b>	<b>7</b>
3.1	Identifying, collecting and creating data	7
3.1.1	(Inter-)active approaches to data collection	7
3.1.2	Passive-observant approaches of data collection	9
3.2	Delimiting and outlining responsibility and accountability	10
3.3	Reproducing the field	10
<b>4</b>	<b>Data management</b>	<b>10</b>
4.1	Organizing data	11
4.2	Data processing and data sharing	12
4.3	Archiving data	13
<b>5</b>	<b>Data analysis and data interpretation</b>	<b>14</b>
5.1	The risk of analytical bias and perpetuating stereotypes	14
5.2	Analysing empirical data towards outputs for policy and practice	15
5.3	Applying general quality criteria of social science to radicalization research	15
<b>6</b>	<b>Publication of findings</b>	<b>17</b>
<b>7</b>	<b>Concluding remarks and practical steps</b>	<b>18</b>
	<b>References</b>	<b>20</b>

# Navigating a Rugged Coastline— Ethics in Empirical (De-)Radicalization Research

**“Make ethics an integral part of research from the beginning on.”  
(Dechesne 2019)**

## 1 Research ethics in (de-)radicalization research

Ethical considerations play a crucial role in all empirical research, with particular challenges in every discipline: From theoretical considerations, over the planning and conducting of empirical studies, up to data analysis and the publication of results, researchers are always confronted with various situations in which they need to navigate the rugged coastline between ethically right versus wrong behaviors, carefully preserving the equilibrium between, for instance, the protection of research participants and the value of academic insights gained. In empirical (de-)radicalization research, particular challenges arise from the implications that the research process itself, as well as its findings, may have for the safety and well-being of individuals, social groups, and the society at large. Furthermore, empirical (de-)radicalization research is in the spotlight of public attention and may come into the focus of security sector agencies, for example, in the scope of risk assessments (Hoffmann et al. 2017). At a fast pace, politicized topics and research fields become salient and evolve—often carrying high hopes as to their short-term policy and practical output. Additional challenges arise from broader societal developments such as technological advances and the access to big data, and debates about open science, developments which are not limited to but also concern (de-)radicalization research.

Applying standards of good scientific practice is generally rather straightforward where rules and regulations are spelled out, and where technological procedures of data management are already established. Ethical guidelines and practice support are the more required where our work reaches into yet unregulated realms and makes use of new technological features, for example, in data collection. At present, guidelines on research ethics in general (Deutsche Forschungsgemeinschaft, DFG, and Leopoldina National Academy of Science, LNW 2014) or online research in particular (Eynon, Fry & Schröder 2008, Tschewinka 2014) do not account for these specific

challenges of (de-)radicalization research. More specific contributions (Mahlouly 2019, Hutchinson, Martin & Sinpeng 2017, Marwick, Blackwell & Lo 2016, van Gorp 2013) are rare and not often shared across disciplinary boundaries (Hutchinson, Martin & Sinpeng 2017, Marwick, Blackwell & Lo 2016, Winkler 2018, van Gorp 2013, van Gorp & Feedes 2013). Yet, research in the field of (de-)radicalization is ‘interdisciplinary’, raising the need for common ground on which research teams from different disciplines can build on.

Researchers need to act responsibly to protect vulnerable persons who participate in or are affected by their research; they need to be mindful of both, and their social environment, while also being mindful of their own exposure. Researchers in (de)radicalization research are in contact with multiple actors and stakeholders, including youth and young adults, individuals at risk, their families, educational staff and counselors, but also police services, judges and courts or policy-level institutions. This creates a context where different personal concerns and institutional mandates may converge and potentially lead to tensions and conflicts of interest that need to be resolved. At the same time, researchers conducting interviews in the field, for example, may take on an exposed role in a contested field and therefore encounter threats by individuals or groups that are connected to a radical scene and who may take a negative interest in both, the research and the researcher.

In the quest to standardize and professionalize ethical practices of academic research, a number of scholarly books and practitioners’ guidelines are dedicated to fundamental questions of moral responsibility (Forge 2008, Briggie & Mitcham 2012) and autonomy (Kämper 2016) reflected in scientific standards and guidelines of ethical practices in data collection and analysis (Van Gorp & Feedes 2013, Roth 2005, Deutsche Forschungsgemeinschaft [DFG] and Leopoldina National Academy of Science [LNW] 2014). Others address questions of normativity (Unger 2014), the specifics of ethics and data protection

in Internet research (Eynon, Fry & Schröder 2008, Golla, Hofmann & Bäcker 2018, Tschewinka 2014) and (big) data management (Boellstorff et al. 2012, Ess 2002 Markham & Buchanan 2012, Rieder & Simon 2017, Ebel & Meyermann 2015, Meyermann & Porzelt 2014, Zimmer & Kinder-Kurlanda 2017), whereas clinical research (Wendler 2017, Wendler & Ried 2017) has provided transferable knowledge on ethics in human-related research. Yet, in the case of empirical (de-)radicalization research, transferring standard practices requires further adaptation, as we argue in the following sections.

Drawing on prior work and the above-mentioned interdisciplinary workshop with 26 experts from social sciences, law and the humanities, this paper aims at establishing common ground and constitutes a first step to what we hope will become a continuing discussion on the subject. In the following sections, the argument is developed along the empirical steps of a generic research process, covering (1) Research context and project set-up; (2) Data collection, (3) Data management; (4) Data analysis and data interpretation; and the (5) Publication of results. In each section, the specific challenges of the respective step are highlighted and discussed as to possible responses. Finally, the conclusion summarizes best practices that may serve as a starting point for disciplinary refinement within research projects in this field.

## 2 Research context and project set-up

Radicalization is a problematic concept that is increasingly criticized within the (de-) radicalization research community (Logvinov 2018, Schmidt-Kleinert 2018, Jukschat & Leimbach 2019). Though widely used, the term lacks clarity and, therefore, analytical potential. Although its meaning is ambiguous and definitions vary, the concept of radicalization tends to individualize the problem and implicitly conceptualizes the process of radicalization as linear and determined. This is already reflected in the titles of radicalization models, for example, Borum's (2011) "Four-Stage Model", Moghaddam's (2005) "Staircase" or McCauley and Moskalenko's (2008) "pyramid". The most widely shared understanding of "radicalization" is that of a process through which people become violent "extremists", whereby, similarly to that of radicalization, the terms extremists and "extremism" are subject to critique: they are both imprecise, judgmental, and normatively connoted and, therefore, orientate scientific, political and public discourses. When used in political contexts, radicalization becomes a categorical term of security policy that distinguishes "non-radicals" from "radicals" or, more specifically,

ly, the 'deviant' from the 'norm' that eventually poses a threat to society (Schiffauer 2015). Implicitly, the conceptualization of radicalism and extremism as fringe phenomena denies extreme attitudes in the mainstream (Oppenhäuser 2011, Falter 2011). This perspective is compounded by an almost exclusive use of the term radicalization in the context of Islamist radicalization (Toprak & Akkus 2019). This not only results in tendencies to overlook or trivialize right-wing extremism (Schmidt-Kleinert 2018), it also affects the public discourse on Islam and Islamophobia in Western societies (Amir-Moazami 2018). Researchers need to acknowledge the profound ethical implications of their research.

The epistemic foundations of a research project require careful thought and critical review. Decisions about the theoretical terms, conceptions and research questions of a project can already have a severe impact on the life of the studied individuals (de Koning, Bartels & Koning 2012). Research projects are part of a process of knowledge production that, in and by itself, constructs the social world. Research projects operating with concepts of "radicalism", therefore, inevitably take part in a process in which social categories are not only described but also co-constructed (Hummel et al. 2016). The mere definition of the term "radical" at the outset of a research project already shapes expectations and may impact the public perception of who is, and who is not, a radical. This could, subsequently, lead to discrimination and social exclusion (Hummel et al. 2016). Related to that, research participants may be concerned about observation and prosecution by state agencies if they participate in the research. If researchers are not transparent about their professional role, this might cause fear and suspicion among research participants or vulnerable communities (Amir-Moazami 2018, Toprak & Akkus 2019). In both, interaction with research participants and public communication, it is hence important to be transparent about project funding and partner institutions.

### 2.1 Empirical (de-)radicalization research in context

Two contextual factors in (de)radicalization research need to be considered for the project setup and the specification of research questions. The first contextual factor concerns a strong political interest in the findings, the second, resulting therefrom concerns the emphasis on and expectations of the practical use and benefits of (de-) radicalization research for policymaking. As a result, over the past years, policy-driven funding for (de-)radicalization research has substantially increased, particularly in European countries (Wehrheim 2018, Teune & Ullrich 2018). Nowadays, a substantial part of policy-related security sector and radicalization research receives funding

from state agencies—in some cases, research consortia or thematic networks even include operational branches or internal research departments of executive institutions, or even intelligence agencies (de Koning, Bartels & Koning 2012).

These context factors set challenges for academic research that researchers and state agents alike need to be aware of. First, the framing of research funding within policy programs may lead to revised criteria for and decisions on financial support to research: (Implicit) criteria defining a project's legitimacy and relevance for policy development might replace the assessment of theoretical and empirical soundness and a project's epistemological scope. Such a paradigm shift would put at risk basic principles of academic research. Second, concerning research cooperation between state agencies and academic institutions, the involved stakeholders need to keep in mind that the functional logics of the sectors are juxtaposed to one another, as concerns their mandate, accountability structures and their internal organization.

For the organization of the research process, from procuring the equipment and sharing empirical data, to the organization of meetings and the publication of results, this constitutes a challenge that requires continued attention and exchange. For all project partners, written cooperation agreements that cover all substantial areas of good scientific practice are most helpful since they detail responsibilities and expectations, and secure the buy-in from institutional hierarchies.<sup>1</sup>

## 2.2 Awareness and transparency regarding public and private obligations

In the field of (de-)radicalization research, scientific knowledge production is often intertwined with the production of security knowledge. Using the concept of “(radical) ization” can quickly lead to research questions that deal primarily with security issues. Researchers should be aware that projects examining, for instance, the radicalization potential of certain living conditions or groups produce knowledge that can—and most likely will—be used by security agencies. In this respect, the projects contribute inevitably to a securitization of social life in Western societies (Singelstein & Stolle 2012). Increasingly, (de-)radicalization research is further used to serve prevention purposes and, thereby, becomes an overarching mode of future-management (Bröckling 2008).

1 This similarly applies to research cooperation with the private sector. The monetization of research results touches upon another dimension.

Both, the securitization of (de-)radicalization research and the increasing dependence on third-party funding create dynamics by which researchers risk losing sight of their professional roles. Dechesne (2019) emphasizes that researchers may fulfil different roles in a given research context and should be mindful of clarifying in what capacity they present themselves: the role of the public or private person, that of an employee of a research institution and that of a local community member, may not always be separable. This goes, in particular, in situations, where the failure to comply with legal obligations constitutes a criminal offence. For most EU-countries, this applies, for example, to denial of assistance<sup>2</sup>, the obligation to report planned crimes<sup>3</sup> or any threat to a child's welfare. To avoid this happening and provide appropriate guidance to project staff, it is highly recommended to discuss and develop standardized procedures for cases where researchers receive data on, or witness illegal or dangerous situations, and establish distinctive referral procedures to psychologists or the police in advance.<sup>4</sup> Ambiguous behavior may impact and, in the worst case, delegitimize research. It is therefore important to regularly reflect on the boundaries of our respective public and private speaker positions.

We suggest that researchers can check their main roles by asking themselves the following questions:

(1) Can I ascertain that I produce rigorous, structured, and confirmed knowledge that may be communicated and proofed by others and that, therefore, aims for intersubjectively comprehensible knowledge of objective validity (the scientific role)? Or, (2) do I try to provide new information about current events of general interest? (This would be one of the main functions of journalism) (Weischenberg, Malik, & Scholl 2006). Or, rather, (3) am I trying to change (societal or political) conditions, for instance, because a group is treated unfairly? (This would be a goal of collective action) (van Zomeren, Postmes & Spears 2008). Or, finally, (4) does my project strive to implement legal conditions consistent with the general law? (This would be the mandate of the executive institutions in a state).

## 2.3 Mapping the field and determining operational requirements

(De-)radicalization research confronts researchers with specific challenges—amongst others the regular engagement of researchers and participants with security

2 In Germany, for example, this is §323c StGB (Strafgesetzbuch, German Criminal Code).

3 For Germany, § 138 StGB.

4 See Marwick, Blackwell & Lo (2016) for further guidance on risk assessment and institutional awareness in “risky research”.

agencies and research conducted in securitized contexts. Further to reflecting on the different roles that may affect the research process, Dechesne (2019) suggests conducting a mapping of the field to identify relational interdependencies of actors, institutions and agents involved in the research and their—implicit and explicit—expectations towards the project. Such a mapping exercise helps to understand contingencies and allows to address ethical concerns. These interdependencies may be visualized as suggested below (Figure 2.1) along relational dependencies and institutional hierarchies. Such a systematic overview helps to depict challenges and risks emerging on all relational dimensions at an early project stage and offers the possibility to include perspectives of a diverse set of partners (e.g., via a stakeholder exchange).

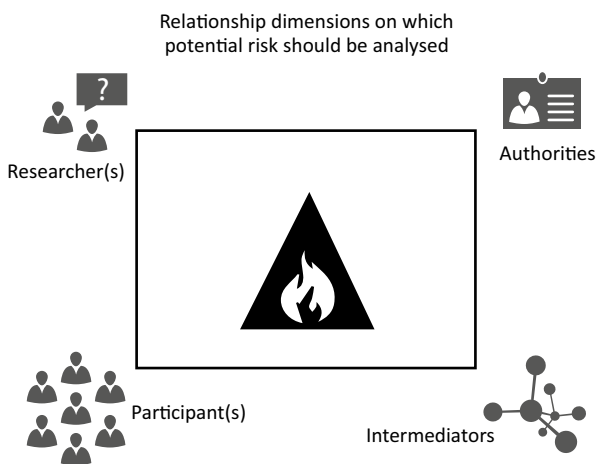


Figure 2.1. ‘Mapping relational dimensions and risks’ (Based on the ‘Safety and security mapping’ of the H2020 project DARE ‘Dialogue about Radicalisation and Equality’)

Such mapping also allows updating the current interdependencies in the course of the project and, thus, accounting for changing requirements due to an evolving field of research changes, for example, after policy changes, as a response to new technologies or a changing security situation.

## 2.4 Setting up accountability mechanisms

In light of the complexity of planning and implementing research projects in social sciences, projects that operate in sensitive contexts and aim to ensure high standards of internal and external accountability are well advised to ‘discharge’ part of their responsibility by setting up internal review mechanisms. Such a mechanism may, for example, consist of a small board of three to five internal and

external colleagues (knowledgeable peers), who convene regularly (e.g., once or twice a year), or on an ad hoc basis in case of need, to review and validate ethical standards in operational proceedings and the research design, access to the field or any other issues the team of researchers feels need to be discussed. While codes of ethics are part of most professional associations’ constitutional framework (Deutsche Forschungsgemeinschaft 2013, American Psychological Association 2016) and internal review boards become more and more common in fields such as psychology and communication, a systematic implementation of ethical standards at the project level or internal ethical review boards are not yet standard practice in social sciences.

In the expert’s workshop as well as within the wider network of participating researchers, many colleagues reported on various project-related arrangements they developed to cover the need for ethical guidance and counselling. In addition to formal advisory boards, the described practices included peer-to-peer as well as professional supervision to cope with psychological pressure or the establishment of peer support networks to share experiences. In some instances, universities make psychological counselling available to their staff and provide structures within their occupational health management. To date, professional supervision of research teams working in sensitive contexts and lacking access to adequate university-bound support structures is funded only insufficiently, if funded at all (Mahlouly 2019). To raise awareness of the issue, researchers may want to include the cost for the use of case networks and the development of team support structures (e.g., supervision/retreats) in their budget.

### *The litmus test of universality, fairness and transparency*

As a “fast check” of one’s own research practices against ethical benchmarks of universality, publicity and fairness, Hünler (2019) suggests to pose the following questions: Could my research practice be universal? That is, (1) would I recommend this course of action to anyone else in similar circumstances? Moreover, (2) would I condone my behavior in others? Could my research practice be made public? In other words, (3) would I tell other researchers what I intend to do? (4) Would I be willing to have my actions and the rationale for them published on the front page of the local newspaper or reported on the evening news? Is my research practice fair? That is, (5) would I treat another participant, independent of his or her status, in the same situation differently?”



### 3 Data collection

**“Freedom of research also means freedom to not conduct certain research.”  
(Hünler 2019)**

Once the research context is defined, and the operational setup of the project is underway, the formulation of research questions further determines the empirical field of research and narrows down methods of data collection. Both, the ontology of the field and methodological questions (e.g., what kind of data sources are available, what kind of data is to be collected and how?) are usually sharpened and refined in an iterative process as the work evolves. Beyond specific requirements of each scientific discipline, ethical considerations in the process of data collection mostly concern the principle of ‘doing no harm’ (Anderson 1992). to others by research interventions, and by “striving for beneficence and nonmaleficence” (American Psychological Association 2016, p. 3). In most cases, researchers do not remain at the periphery of their field but leave imprints in it, for example, by interactions with counterparts and participants, or by shaping the overall interpretation of the topic. They thus take an active role in the construction of the field and this possibly even beyond the mere period of active data collection.

By consequence, ethical concerns in the process of data collection closely relate to preserving individual self-determination and autonomy as well as safeguarding personality rights and ensuring the personal safety of all involved persons (for a more general discussion of current privacy and data protection regulations see section 4.1).

Against this background, the following questions are central to ensuring a critical screening process:

1. What are the legal, organizational and normative determinants, constraints or vulnerabilities that govern the research field? How do they determine where (access) and how (method) data is collected and produced?
2. How do participants agree to take part in the study? Is an explicit consent to participation and the processing of data possible?
3. What is the impact of data collection on actors, agents and dynamics in the field? To what extent are things like post-intervention support or risk mitigation needed?

The following sections give details of the proceedings for ethical compliance at this stage of the research process and provide further guidance to self-assessments within project contexts.

#### 3.1 Identifying, collecting and creating data

To determine whether or not it is ethical to collect data in a specific field of research, it is necessary to assess the method (that determines which data is collected in what manner) against the context parameters and the constitution of the field. This equally applies to quantitative and qualitative methods, as for both approaches, personality rights, self-determination and personal safety considerations concerning research participants remain relevant throughout the process of data collection. We propose to discuss ethical concerns regarding the identification, collection and production of data by differentiating (inter-)active approaches on the one hand, and passive-observant approaches, on the other. While (inter-)active approaches involve, for example, any methods that require personal, verbal or written exchanges among researchers and research participants; possibly participants’ instructions on data collection instruments; experimental settings or any kinds of interviews, to name but a few, passive-observant approaches include the establishment of document or media corpora, protocols of non-participant observation, secondary or meta-data analyses, etc.

The distinction of data collection processes along these two categories, so our argument goes, allows carving out the differences in regard to provisions of privacy and data protection. More specifically, it allows researchers to self-assess to what extent the data they are about to collect and process:

1. requires informed consent of participants or necessitates ex-post communication on aims and implementation of the study;
2. relates to the public or private sphere and carries specific authorship or ownership rights;
3. makes provisions for opting-out of the study/research possible; or
4. necessitates financial or material compensation of participants.

##### 3.1.1 (Inter-)active approaches to data collection

Data from (inter-)active approaches can be created through qualitative (e.g., interviews or focus groups etc.) as well as quantitative research (e.g., surveys or experiments), both online and offline. Depending on the field of research, cultures and contexts (Markham & Buchanan 2012), ethical standards of data collection vary, for example, with respect to the required anonymity of research participants. We would like to draw on current practice in psychological research, where ethical standards on data provided by human subjects require the researcher to adhere to the criteria of (a) *informed consent*, (b) the



avoidance of *unintended side-effects* of data collection, and (c) *incentivization*.

**Informed consent.** *A priori consent* implies that research participants are fully aware of (a) the aims of the research project and its financial sources, (b) the answers or actions required during data collection, as well as (c) the treatment of their data after data collection (see also section 4.3). Ethical guidelines for social sciences research<sup>5</sup>, as well as the EU General Data Protection Regulation (§13, GDPR) considers informed consent a necessary precondition for creating data (Schaar 2017). Getting informed consent for (de-)radicalization research projects often needs time for building “networks of trust” (Dechesne 2019), particularly, where vulnerable groups (e.g. minors or minority groups) are part of the target group. In line with the German Science Foundation DFG’s affirmation for honesty in “oneself and towards others” as a most crucial value within the scientific process (Deutsche Forschungsgemeinschaft [DFG] 2013, p. 67), transparency about one’s research aims and decisions is a moral obligation both towards the scientific community and one’s participants. Article §13 of GDPR (§13) requires that participants can contact the researcher directing the study.<sup>6</sup> “In an exemplary manner, the ‘Dialogue about equality and radicalization project’ (DARE) uses an information sheet outlining the purpose and procedures of the conducted research, which provides full disclosure and has a reference to the consortium website and a contact address” (Dechesne 2019).<sup>7</sup>

However, not all research allows for a priori transparency, in particular, when such information is likely to bias participants’ answers. If it is necessary to conceal research aims, a combination of a priori information for obtaining consent and a post hoc debriefing that enables research participants to retract their data is considered acceptable (BPD & DGPS 2016). Researchers can include a similar “opt-in” option in (pseudo-)anonymized questionnaires or verbally in an interview situation. An accordant debriefing can be implemented in qualitative and quantitative studies and should allow for the immediate deletion of collected data consistent with the “right to deletion” (§17, GDPR)—although there are exceptions for scientific archival purposes when deletion “is likely to render impossible or seriously impair the achievement of the objectives of that processing”. This is particularly likely in the context

of pseudo-anonymized data<sup>8</sup>, where the right of deletion cannot be executed meaningfully (see section 4.3).

**Avoiding unintended side-effects.** (Inter-)active data collection allows researchers to execute certain levels of control over the questions, stimuli, and conditions they confront their participants with. The ethical principle of striving for beneficence and nonmaleficence is the guiding principle here. Yet, implementing this principle in the context of empirical (de-)radicalization research is sometimes more tricky than anticipated. For instance, seemingly “easy” decisions, such as avoiding the exposure to scenes of graphic violence (Rieger, Frischlich & Bente 2013) or removing final scenes of beheadings from extremist propaganda videos (Cottee & Cunliffe 2018, Klonek 2019) used in quasi-experimental research, have been discussed critically as stimulating “curiosity” (Winkler 2018). As another example, innocuous questions about reasons that induced interviewees to join a radical movement or terrorist organization could stimulate rose-tinted memories about the person’s past and therewith impair intergroup relations.<sup>9</sup>

**Incentivization.** Where possible and appropriate, the time invested by an interview partner or participant should be recognized and compensated. This can be done in-kind (e.g. by offering access to the research results, invitation to a transfer event, etc.) or monetarily. In the context of radicalized groups and individuals, however, one might argue that monetary compensation could be used to support ideological groups and their activities. Although it is hard to avoid the misuse of funds irrespective of the research context, the risk of “financing” illegal activities can be a particular concern in the context of empirical (de-)radicalization research. It is necessary to remember here that compensations for participants are usually rather low. However, if individual compensation is a problem in this field of research, at project level, one strategy for compensation could be to donate funds to a charitable or other civil society organization that works on democratic grounds and supports moral values promoted by the interview partner(s). Similar considerations apply for providing funds to research participants in powerless situations such as minors, detainees, etc.

5 For Psychology, see, for example, American Psychological Association (2016); BPD & DGPS (2016); for Sociology, Deutsche Gesellschaft für Soziologie (DGS) (2017).

6 This level of transparency is also compatible with recent open science movements, such as the call for pre-registration.<https://osf.io/prereg>

7 <http://www.dare-h2020.org/>

8 On the definition of pseudo-anonymization, see §3, GDPR and <https://gdpr.report/news/2017/09/28/data-masking-anonymization-pseudonymization/> (last accessed, November 18, 2019). <https://gdpr.report/news/2017/09/28/data-masking-anonymization-pseudonymization/>

9 For a study about the relationship between such “collective nostalgia” and hostile intergroup attitudes, see Smeekes, Verkuyten & Martinovic (2015).

### 3.1.2 Passive-observant approaches of data collection

Data collected by passive-observant approaches can be obtained offline or online and analyzed qualitatively and/or quantitatively. For data generated by methods such as ethnographic or corpus analysis, ethical standards generally focus on questions of (a) *privacy* and (b) *acknowledgement of data sources*, along with more specific needs for ensuring (c) the *safety* and *security* of researchers themselves (particularly, when it comes to research with potentially violent groups).

**Privacy.** In contrast to (inter-)active approaches, in passive-observant approaches, it is not possible to secure a priori consent. To determine whether or not researchers can assume that any author or data owner have given their consent, it is helpful to distinguish whether data relates to the public or the private sphere (Markham & Buchanan 2012). Public mass communication—articles published in a newspaper or a propaganda-magazine—is usually considered unproblematic for analyses, whereas interpersonal conversation (for example, in a home or closed family chat) relates to the private sphere and is given special legal protection. While this distinction seems to be quite obvious offline, the limits of mass communication and interpersonal communication become blurred in social media (Walther & Valkenburg 2017). Here, individuals might consider their (public) tweets as private (for much-needed insights into user perspectives in this context, see Williams, Burnap & Sloan, 2017), and classify social media platforms as semi-private spaces (Neubaum 2016). The resulting challenge has already stimulated some debate in the context of empirical (de-)radicalization research (Buchanan 2017). The increasing relevance of “dark social” platforms and encrypted messengers for the general public (Newman et al. 2019) and extremists suggests that semi-private spaces will remain a crucial field for future (de-)radicalization research (Bloom, Tiflati & Horgan 2017, Neumann et al. 2018). As an attempt to solve the inherent ethical challenge, Golla (2019) argues that research may be considered ethical when the social value of the results outweighs the intrusion. Taking medical research as an example, a further justification might need to be given when not only third parties but also the researched individual (data owner) him- or herself are expected to benefit from the research (Wendler 2017).

**Acknowledgement of data sources.** Data access is a challenge in all empirical research and, when given the option, researchers may prefer to choose to collect data in an easy-to-access field rather than in a closed-up one. Particularly in the case of publicly available data from online sources such as Twitter, VKontakte, Facebook and others,

the easy access to data has led to a shift in the focus on data collection for many research projects (Kaiser 2018). Regardless of the origin of data and the effort with which it can be collected, however, ethical standards require transparency and adequate documentation about how and where data was collected. The ‘free’ availability of data does not relieve researchers of the obligation to acknowledge sources via adequate citation and attribution of authorship (Markham & Buchanan 2012). In the case of data from propaganda documents or media outlets of terrorist organizations, the format by which sources are acknowledged needs to be chosen with care and accompanied by a disclaimer as to contents, or else, researchers risk fueling violent competition for attention by extremist movements or terrorist groups (Kruglanski et al. 2018, Koloma Beck & Werron 2013) [see also section 3.3 and Chapter 6].

**Security.** Relating to the issues of confidentiality, integrity and civic obligations, researchers might need to decide whether to reveal their identity or conduct research incognito. Researchers studying risky topics such as (de-)radicalization need to watch their own security and the security of their team members (Marwick, Blackwell & Lo 2016). In consequence, some (de-)radicalization researchers choose to stay anonymous when monitoring violent extremists’ online communication channels (Bloom, Tiflati & Horgan 2017) or offline networks (Ebner 2017). From a technical point of view, the use of fake identities is rather simple. From an ethical perspective and regarding research methods, however, it can be very problematic as it violates the already mentioned principle of honesty. Similarly to other decisions that concern a derogation from ethical practices, the decision to use fake identities for safety reasons needs to be carefully justified and weighed against the epistemic value of the research (see section 3.1).<sup>10</sup> Here, the principle of proportionality as well as the consideration of explicit or implicit consent, as discussed in the next section, are helpful.

<sup>10</sup> Methodically, the use of fake accounts is also concerning in regard to the metrics of accounts, chat groups and websites as it is no longer possible to estimate whether a group of 300 persons actually contains third party observers or original members and to ascertain the origin of a communication. As to the criminal-legal perspective, the infiltration of online groups can become an issue where consequences of communication can no longer be contained, for example, where chat partners might feel encouraged to pursue violent acts due to ambiguous communicative behavior on behalf of the rest of the group.

### 3.2 Delimiting and outlining responsibility and accountability

In light of their social responsibility (§1 para. 3 DGPUK 2017), researchers are accountable for their actions and have moral obligations to act responsibly, particularly towards their research subjects, to adhere to the law (American Psychological Association 2016), to promote fairness (DGPUK 2017) and—more generally—human rights (Markham & Buchanan 2012). These obligations also need to be considered when establishing research instruments—including the consideration of unintended side effects—and inform strategies for dealing with critical incidents (see also section 2.3). Accordingly, decisions can be easily combined with other best practices such as the discussed risk analysis, routines of pre-registration, including the justification of meaningful effects sizes (Anvari & Lakens 2019) and the planning of one's sample size in qualitative research (Haven & van Grootel 2019).

As a minimum requirement, an ethical research design needs to ascertain that (1) research participants may quit whenever they feel uncomfortable (particularly in the case of detainees or participants that are governed by other dependency relationships) without having to fear negative consequences (including losing one's incentives); (2) participants can contact the research director and/or his or her focal point.<sup>11</sup> Besides, (3) empirical (de-) radicalization research may require additional safety nets for further advice, information or referral, such as, for instance, including contact information to (de-)radicalization experts, psychological care, or an extensive debriefing, allowing the participant to voice potential negative sentiments before incentives are provided. From our own work, we found that sharing experiences with participant groups and collecting background material is extremely helpful for the development of safety nets and awareness of potential issues. To give an example: Teachers, security officials or teenagers tend to judge media content quite differentially from each other, and what seems innocuous in one cultural context might have diametric effects in another. Talking to people outside of one's narrow "research bubble" or the literal "ivory tower" in advance can help to become aware of such pitfalls (e.g., through regular accounts to and exchanges with the advisory board suggested in section 2.4).

11 These criteria are also standards set by the EU-GDPR and ethical guidelines of professional associations, for example, American Psychological Association (2016).

### 3.3 Reproducing the field

Even when collected data refer to propaganda material collected online only (i.e. there is no direct interaction with human participants), viewing, downloading, or bookmarking accordant content on platforms with interaction-based algorithmic recommendation systems (i.e. social media sites) inevitably fuels the "success" of accordant materials at least in the "eyes" of the recommender algorithms. Restricting the number of clicks on extremist material is thus well advised, although it might require downloading and sharing accordant material within research groups. Since the (public) dissemination of extremist propaganda is against the law in many countries including Germany, storing and sharing of accordant material needs to be done with care and according to high data protection standards. Besides, particularly in the context of (de-)radicalization research, material collected and/or provided for research purposes may violate national laws. Another strategy to avoid the inflation of interaction is to cooperate with intermediaries outside of research, e.g., platforms (see, for instance, the Facebook SoSci One or Crowdtangle grants, Twitter's academic partnership, or alphabet's "moonshot countering violent extremism" branch), security agencies (e.g., for file access, to reach out to incarcerated interview partners), NGOs, religious organizations, or business partners. Although such cooperations are extremely valuable, and some of the authors have substantially benefitted from them, we are also aware that they need to be constantly reflected to ensure independency of research, particularly in light of the securitization phenomenon discussed in Chapter 2.

## 4 Data management

**"Data protection is a resource of trust."  
(Golla 2019)**

Data management refers to the organization, processing, sharing, storage and archiving of 'created' and 'observed' research data. While data management and data protection are oriented toward fulfilling ethical and professional standards regardless of the discipline, specific legal and technical requirements may apply to online and offline (de)radicalization research. Building on key questions we have encountered in our own research, the next section offers some guidance and possible response to these specific challenges. The sections are developed along the aforementioned elements of data management—from organization to archiving—and focus on legal and technical aspects respectively in each section.

## Challenges

For European researchers, in particular, it is sometimes hard to keep up with the evolving EU and national legal regulations as well as with ethical guidelines of professional associations and research institutions. Also, evolving technological innovations allow for new approaches to conducting, sharing, processing and analysing research data, but may also lead to yet unregulated realms of data management. Particularly in a sensitive field such as (de-)radicalization research, there is an inherent tension between the values of open science and privacy protection.

Related to that, researchers might find themselves in a double-bind situation as regards their obligation of confidentiality towards respondents and—depending on national regulations—their legal obligations to disclose information on severe criminal offences or to testify before a court.<sup>12</sup>

Concerning decision-making processes, some professions are bound to institutionalized codes of conduct and legal guidelines, as are, for example, psychotherapist<sup>13</sup>, which help them navigate accordant questions. In contrast, other professions, such as some in social sciences, operate in a much more fluid and contingent field, which increases exposure and ambiguity. For researchers in Germany and the United Kingdom, for example, personal liability regarding data management and/or the disclosure of information is regulated by different laws.<sup>14</sup>

### 4.1 Organizing data

In many research contexts, research institutions, research partners, beneficiaries and participants demand that the researcher provide a written commitment to data protection and privacy regulations. Research institutions provide different infrastructures to support researchers in writing such a concept. Usually, researchers can use the support of the institution's legal department, research data management services—often attached to the library—or decentralised support units in departments or faculties. It is also worth checking, whether one's university provides appropriate training for doctoral students or postdocs. We strongly advise involving local contacts for data protection at an early research stage.

One of the best ways of dealing with data organization and planning ahead is to prepare a project-specific data protection policy ("*Datenschutzkonzept*" in German) at the outset of a research project. This allows thinking through the technical set-up, legal regulations and the ethical code applicable to the project and, thereby, establishing basic rules for data collection and management. In many research environments, such a data protection policy note is already mandatory. A suggested structure for such a concept is presented in section 4.2 below. The data protection policy should integrate the legal requirements as well as technical aspects of data management.

In projects that are currently conducted in the EU, the *General Data Protection Regulation*<sup>15</sup> enacted on May 25, 2018, provides most likely the most important normative framework to privacy rights and data protection.<sup>16</sup> National legislation and policies that apply specifically to scientific research also need to be checked. In Germany, for instance, relevant institutions, working on data protection and ethics are the National Office of the Ombudsperson for Data Protection<sup>17</sup>, the sub-national Ombudspersons (*Landesdatenschutzbeauftragte*), the Commission for Data Ethics at the Ministry of the Interior<sup>18</sup>, and the institutional focal points for data protection of public and private research institutions. In some cases, the legal departments of the research institutions also provide guidance and advice as do university-based focal points for research ethics or institutional ethics committees. Also, international and national professional associations and advisory committees provide useful guidance notes on the application and transfer of legal frameworks to scientific research. In Germany, the Rat für Sozial- und Wirtschaftsdaten (RatSWD) constitutes a standing advisory committee to the government on issues of data management in social sciences and also publishes position papers, for example, on data protection.<sup>19</sup> The legal framework of data protection has an impact on the *technical and procedural* organization of data.

Once the empirical field of research is determined and evolves as researchers immerse themselves into data collection, the more intuitive parts of data management generally relate to the

12 See, for example, University of Sheffield, Policy Note No. 12, Research involving illegal activities, at [https://www.sheffield.ac.uk/polopoly\\_fs/1.112762!/file/Research-Ethics-Policy-Note-12.pdf](https://www.sheffield.ac.uk/polopoly_fs/1.112762!/file/Research-Ethics-Policy-Note-12.pdf); Lowman & Palys (2001).

13 In Germany as per §§203 and 138 StGB respectively.

14 For Germany, these are §§1,2 VerpflG, §5 BDSG, and §§203-205, 353b StGB. For the United Kingdom, the Terrorism Act (2000) specifies a "Disclosure of information: duty" in section 19 (1), see <http://www.legislation.gov.uk/ukpga/2000/11/section/19>.

15 GDPR at <https://eugdpr.org/>.

16 Beyond the EU's geographical scope, the OECD Privacy Framework (2013), under revision as of December 2019, constitutes another relevant policy framework.

17 Bundesdatenschutzbeauftragte/r at [https://www.bfdi.bund.de/DE/Home/home\\_node.html](https://www.bfdi.bund.de/DE/Home/home_node.html).

18 Datenethikkommission at <https://www.bmi.bund.de/DE/themen/it-und-digitalpolitik/datenethikkommission/datenethikkommission-node.html>.

19 <https://www.ratswd.de/themen/datenschutz>.

- I **data format** (e.g., audio files, transcripts, video sequences, photos, digital pictures, rich text, document scans, experimental and survey data, etc.);
- I **software** needed to structure, organize and eventually analyze the primary or secondary data (e.g., statistical programs, quantitative or qualitative analysis tools like Atlas.ti, MaxQDA, F4; media player, SQL/postgreSQL databases);
- I **hardware** needed to store data to and access data from for working sessions (see ‘Data Processing and Data Sharing’ below); and
- I arrangements for **data archiving or secure deletion**.

To sum up, some of the major challenges facing the organisation of data are:

- I An increasing obligation for researchers to observe legal regulations and ethical guidelines;
- I At the same time, often a practical lack of knowledge and training about these obligations or recent changes;
- I Lacking juridical support or advice to the researcher in the research process;
- I Legal protection on privacy and data protection may allow for the processing of data, regulations may, however, still conflict with the researcher’s professional ethics”

#### 4.2 Data processing and data sharing

From a legal perspective, any import of research data into a software is already considered as data processing and thus falls under regulations of privacy and data protection.<sup>20</sup> Researchers need to be aware that this can even include copying data, e.g. from social media, via the copy-and-paste option into any other software to store it. Also, any sharing of data is data processing.

Thus, the first step in protecting data from unauthorised access is to secure privacy rights. As to storage, it is important to know that EU privacy legislation only accounts for data stored on servers in the EU. Yet, in practice, a number of cloud services are provided by firms registered in the United States, where the legal situation is different and standards for data protection are much lower. One notable difference is that government agencies may get access to data stored on US servers without the knowledge of the data owner. Using EU-based solutions might not always be possible: cloud solutions like ILIAS or Power Folder usually provide a description of the kind of data allowed for storage on these platforms and indicate that

the storage of data containing private information usually is prohibited.

In line with EU legislation, researchers are obliged to establish procedures to control and document access to data that contains private information. To this end, data security tools, such as firewalls on internal networks, or commercial, respectively freeware, encryption tools may be used. To control physical access, many institutions working with sensitive data have safe rooms or special archives accessible to authorized personnel only. Here, mobile storage tools (like SSDs, hard drives, USB sticks, etc.) or hard copy documents and other data can be stored, for example, in steel cabinets. From our own experience, it may further be practical to establish stand-alone workstations without Internet connection or connection to internal networks to secure authorised access and maintain high data security standards throughout processing and analysis. These workstations could also be used to store data.

Since sensitive data requires special technical equipment, it is necessary to include the cost for additional technical equipment into project budgets. In some of our projects, we worked with a substantial number of court files, parts of which we scanned for the analysis. Since most network scanners store all documents on an internal memory that cannot be accessed and erased, one institute chose to buy a separate copy/scan machine that was available at a local workstation; another institute worked with a mobile scanner that had no internal memory. To minimize the risk of losing files and mobile storage tools in cases where cooperating institutions are physically remote, it is advisable to limit physical transportation and prioritize personal handover that can be documented and signed-off. Some institutions, mostly of the private sector, have access to highly securitized clouds or may recur to well-protected internal servers that may serve the purpose of data transfer.

We followed and valued the standard procedures of processing and storing of sensitive data in the above-mentioned research projects that dealt with court files, i.e. the “data life cycle” that is described in the following:

<sup>20</sup> See § 4, (2) and (6) GDPR and Recital 26, GDPR at <https://gdpr-info.eu/recitals/no-26/>, last accessed, November 19, 2019.



### Schematic Data Life Cycle

PROCESSING DATA	STEP 1	STEP 2(a)	STEP 2(b)	STEP 3	STEP 4	STEP 5
Technical steps	Secure storage of original data	...	Make a working copy on a copier or scanner, which has not got any connection to the Internet or intranet	...	...	<ul style="list-style-type: none"> <li>• Destruction;</li> <li>• Archiving of original data or working copies</li> </ul>
Data life cycle phases	1. conducting sensitive data	2. exchanging sensitive data	3. importing sensitive data into analysis software	4. analysing sensitive data	5. publishing sensitive data	6. finishing a project
Possible risks	<ul style="list-style-type: none"> <li>• unauthorized access to, dissemination of or loss of personal or customizable data (phases 1-4)</li> </ul>					
Possible solutions	1. limited group of people with authorized access (access control);				...	1. secure destruction of data;  2. personal handing over <ul style="list-style-type: none"> <li>• Backup-archiving of electronic data at a scientific institution's data processing service center,</li> <li>• Archiving of data on paper at the respective unit of a scientific institution, complying with the rules of good scientific practice</li> </ul>
	2. training on prevention of security issues for authorized personnel;  3. original data are stored in the institution, which applied for access (access control)	2. personal handing over of working copies a) on paper, or b) as a scanned copy on an encrypted volume with the password handed over separately (dissemination control)	2. storage of working copies on an encrypted volume or on paper in a locked steel locker (access control)	2. analysis of data only in a "safe room", on a special computer, which has not got any connection to the internet or intranet (access control)		

### 4.3 Archiving data

From our experience, research institutions handle data archiving very differently. An increasing number of universities offer the possibility of secure archiving, i.e. in line with current data protection legislation, of (digital) research data for the period required as per project regulations. Contacting your own institution's department for digital infrastructure or the legal department can help to obtain specific information on this.

In some cases, it may be necessary either to fully destroy original research data or to partially delete sensitive infor-

mation, i.e. data, which has not been anonymised.<sup>21</sup> For the permanent deletion of confidential electronic data, special software can be used – again, exploiting commercial or freeware options. Further, research institutions may provide a structure for the secure destruction of confidential documents.

21 See also <https://gdpr-info.eu/recitals/no-26/>.



## 5 Data analysis and data interpretation

Once the initial phase of data collection is terminated, the processes of data analysis and interpretation begin. While data sets tend to vary widely across different project contexts, they all require systematic preparation for analysis. The process of data analysis may include data cleansing and data editing<sup>22</sup>, processing of documents and texts in analytical schemes, visualizing video or sound sequences or systematizing interview transcripts—to name but a few. Data does not “give away” the answers to our research questions by itself, but requires methodical analysis and interpretation to decode information and generate knowledge.

When it comes to data analysis and interpretation, the specific issues and challenges that arise in (de-)radicalization research are very much connected to the institutional and conceptual context within which researchers operate (see section 2.1). In our experience, these concern two issue areas that are interrelated: first, the risk of analytical bias and perpetuating stereotypes through insufficient methodological rigour and peer control, and, second, the instrumental analysis of empirical data towards outputs for policy and practice.

### 5.1 The risk of analytical bias and perpetuating stereotypes

To engage in empirical research often means to work with typologies. This is true at different moments during the research process: we are urged to use certain terms when applying for funding, when dealing with beneficiaries or security authorities on an everyday research basis and, in particular, when describing research findings. Researchers need to make a difference, however, between the characteristic style of a research proposal that third parties and possible non-academic boards of funding institutions need to understand on the one hand, and the analytical concepts, typologies and categories that need to be rigorously applied to the data material based on scholarly literature, on the other.

22 The process of data cleansing and editing focuses on the deletion of incomplete data sets, “duplicates” or “irrelevant observations” (<https://elitedatasience.com/data-cleaning>, last accessed November 21, 2019) in line with methodical standards that need to be documented as part of the methodological work. Data cleansing is not in any way related to the deletion of unwanted results or the manipulation of data. Against the background of recurring debates on “fake sciences”, researchers need to make sure they fully comply with ethical standards, document their work and proceed in line with professional standards and, thus, account for their work.

Working with pre-defined concepts, typologies and categories always leads to simplification, for example, when describing specific attributes of individuals or groups; of discourses or sets of behavior. The same is true for the operationalization of theoretical constructs in quantitative research. In projects that focus on the particularly politicized thematic area of (de)radicalization, researchers need to be aware of the fact that simplification on the one hand and politicization on the other may develop mutually reinforcing dynamics, to which their analysis may contribute and foster or reinforce not only stereotypes but also prejudice (Gilks 2019). In analogy to the points raised in section 2.2, researchers are not neutral, but political and social subjects with their own prejudices and belief systems, which, whether consciously or not, may also impact their analytical perspective and their reading of results.

To counter the effects of analytical simplification and prevent the diffusion of blurry concepts or imprecise terms from public security discourses, it is all the more important to maintain academic standards of data analysis and to critically reflect on one’s own position in the process, one’s work and one’s findings (Law 2004). In general, as a matter of high professional standards, researchers need to make sure that the typologies they apply to or develop from the empirical material (Kelle & Kluge 2010) are grounded in that same material, regardless of whether they work with quantitative or qualitative approaches. In other words, if researchers develop typologies, the features for that must either be derived from empirical data (inductive) or need to be confirmed by the data (deductive). If research data does not confirm the features that define a term, it is unethical and against scientific practice not to document and discuss these findings; or to continue promoting unsustainable conceptual approaches.

For one thing, before adopting terms and typologies used in the field and reproducing these, for example, in funding proposals, researchers need to take a critical stance about their empirical reliability and validity. It is good practice and essential to professional research practices to update concepts, approaches and typologies, or discard them if they lack any empirical foundation. For another thing, researchers need to remain cautious not to take interpretative shortcuts to meet reporting deadlines—if results cannot be affirmed with the necessary empirical results (as of yet), this needs to be reflected in the presentation of results.

For qualitative research, in order to strengthen critical reflectivity and attain intersubjectivity—that is, a shared understanding of interpretation and results, researchers may, for example, establish working groups that help them to reflect about normativity and preconceptions that are

inherent to their analytical framework. In our experience, however, ascertaining intersubjectivity does not guarantee full awareness of stereotyping or of one's own embeddedness in racist structures. This is a serious problem, since in (de-)radicalization research, research participants and groups within the field are already exposed to and experience racism on a regular basis. To strengthen critical awareness of hegemonic structures in research designs, a 'decolonization approach' to methods can be helpful (Mignolo & Walsh 2018, on methods Kaltmeier & Berkin 2012, and for a critical discussion of the approach, Barnes 2018). Also, methodical approaches from Critical Security Studies are established practices and immediately apply to (de-)radicalization research as well (Salter & Mutlu 2013, Dixit & Stump 2015).

Last, one trend that can be observed when working on interdisciplinary questions relating to (de-)radicalization is that there is a trend to form a community of practice that has little exchange with academic disciplines and sub-disciplines in which theories and methodologies of (de-)radicalization research are grounded (social psychology, political sciences, criminology, sociology, etc.). This affects knowledge production and peer control and, in conjunction with the analytical shift to policy and practice-relevant outputs, increases the inclination to orientate research at political perceptions of 'problems' or 'world views' or concepts and keywords from public discourses.

## 5.2. Analysing empirical data towards outputs for policy and practice

Conducting (de-)radicalization research under the framework of security-related sciences funds schemes frequently involves a project consortium to which security sector institutions are either associated or in which they may even engage in the lead of the project. Where researchers agree to terms of cooperation with executive agents, it is particularly important to reflect about the interests of all stakeholders, specify terms and concepts, and highlight ethical values and professional practices of their research (see also section 2.1).

At times, researchers experience pressure from funders or beneficiaries to come to analytical conclusions in a format that allows for the formulation of policy recommendations. While this has become a common trend in many areas of science and academia, it is specifically challenging in a field of research that is topical in political debates. What is more, however, is that it should be of concern to researchers when data analysis is framed to provide outputs for policy and practice, and the deeper understanding of the empirical basis is neglected. While it is important to

acknowledge empirical research in policy-making processes in empirical research findings and thereby increasing political legitimacy, it is necessary to keep in mind that providing policy support is neither a researcher's mandate nor at the core of their work. Rigorous empirical research inherently requires time and, time and again, it may be necessary to slow down processes and forgo the speedy production of output to the benefit of more thorough and potentially more far-reaching, substantial findings (Soeffner 2004). This may be difficult to ascertain in field of (de-)radicalization research, where a diverse set of stakeholders engage, each with their own legitimate agenda. This pressure may at times be tricky to handle—it is imperative, however, to stick to academic quality criteria; and in this context, it may be of value here to be aware of the role researchers embody (see. section 2.2).

Another situation where researchers may be asked to provide policy recommendations or feedback to preventive measures occurs in contact with the media. The topical relevance of (de-)radicalization research in current political agendas stimulates the interest of the press and news media in insights into—possibly not yet available—results and progress. Considering the high value of exclusive news, it is also common to receive requests for expert interviews at short notice and in connection with daily events.

While this pressure is tricky to handle, researchers should stick to academic quality criteria and be aware of the role they embody (cf. section 2.2). When responding to such requests, it is legitimate, and even professionally required, to specify whether or not one is competent to speak on a specific subject, which, as a researcher, can only be the case if there is a relevant research record.

## 5.3 Applying general quality criteria of social science to radicalization research

Although there are many different research methods, there are some common quality criteria of empirical social research (Cameron 2011, Diekmann 2004, p. 223). We think it may be helpful to point them out and discuss them in the context of radicalization research.

**Validity.** Research validity is the degree to which a research tool is accurate, that is, the degree to which it measures that which it is supposed to measure (Cameron 2011). This is specifically relevant when using quantitative data. For instance, when speaking about radicalization research, the tag "radical individual" usually carries a stigmatizing connotation. Therefore—specifically when making claims about certain parts of the population's degree of radicalization—, one has to be clear that this is

what it measured.<sup>23</sup> This is different when you are not sure about the topic you are looking at: How can you measure radicalization if the actual meaning is still highly contentious?

**Objectivity.** A lack of objectivity impacts on the legitimacy and scientific value of research designs and, in consequence, forbids drawing more general conclusions from the generated findings.<sup>24</sup> In quantitative methods, objectivity requires a research tool to be independent of the person/researcher who is using it (Diekmann 2004, p. 216). So ideally the questionnaire should produce the same results irrespective of the person who is handing it out. And the analysis of research A and B should obtain the same result. One way of dealing with such challenges could be to have a heterogeneous team of researchers to balance any flaws occurring through the influence of individuals. This is more difficult for qualitative methods and interview settings (Przyborski & Wohlrab-Sahr 2008, p. 40).

**Reliability.** Reliability is a measure for the degree to which results can be replicated when using quantitative methods (Diekmann 2004, p. 217, Cameron 2011). This is not the aim of qualitative methods. Some would say they aim more at reconstructing everyday standards of communication and interaction (Przyborski & Wohlrab-Sahr 2008, p. 39). Others would say confirmability (Guba & Lincoln 1985) is the more appropriate term to describe reliability in qualitative research. It calls upon the researcher to make sure that his or her account of social reality is grounded in social reality. One way of doing so is to validate results in a systematic process with peers. This means, ideally, there is intersubjectivity, which can best be assured by practising reflexivity (see above). Another way of ensuring confirmability is to apply methods of data and researcher triangulation whenever possible, meaning to get different points of data, be it interviews with people from different points of view, be it case files on top of interviews, etc. This again is highly challenging in a field

so full of political debate—because that way the process of interpretation is closely connected to opinions and ideological positions.

**Generalizability.** The generation of knowledge from qualitative and quantitative research very much depends on the level to which findings and results can be generalized into regularities and ‘social laws’ as well as transferred into other contexts. In quantitative approaches, standardized quality criteria for sample size and sample constitution indicate to what degree the findings are significant and allow transferring findings from the examined sample to larger social groups<sup>25</sup>. In qualitative approaches, and depending on the data sets, the generalizability depends on the comprehensiveness and systematics of analysis, as well as the relevance of cases for the broader research question. As an example, we may look at developing patterns and an empirical typology (Kelle & Kluge 2010) of radicalization of individuals from biographical interviews with persons convicted on charges of terrorism. Other challenges could emerge when quantitative data sets include only a small number of people from power minorities/numerical minorities. Data could be used to form misleading conclusions about group differences without ensuring the measurement equivalence between cultural groups (Odağ et al. 2016)—an aspect the authors themselves did not account for enough in some of their early work (Rieger, Frischlich & Bente 2013).

To enable more general conclusions on the relevance, for example, of individual life courses and collective processes, the analysis needs to be robust and contextualized; cases have to be substantiated, must not be anecdotal and, with regard the personal narration of relevant instances in the process, information needs to be triangulated. For interviews, this could be done through case file analyses, or interviews with family members, or the like. Every qualitative method has its checks and balances that need to be maintained and documented systematically. Every researcher needs to pay special care to transparently communicate the (lack of) generalizability and transferability of their findings and results, since the interpretation of results may have a direct impact on public discourse and policy decisions.

23 Goede, Schröder & Lehmann (2019) debated their problems with a scale about radicalization and their realization that a scale they had used did not prove to be useful as, instead of revealing radicalization, it revealed political interest.

24 In the recent past, for example, a specific set of surveys on the prevalence of antisemitism and homophobia in Muslim and Christian groups in Europe (Koopmans 2015) has been discussed controversially. The results of the surveys suggested higher rates of antisemitism and homophobia in the first group. The surveys were heavily criticized as to their design and inherent bias as the target groups were composed in such a way that there were substantial issues to inter-group comparability as the composition of the groups was not representative. Further, the ‘findings’ relating to the groups per se could not be established as group-specific, which is a substantial issue both for the quality and ethical standard of the contribution. Yet, the results of these surveys continue to be discussed in some forums as substantial empirical research.

25 On generalizability and transferability in qualitative and quantitative methods, see Polit & Beck (2010). For quality criteria, see Andrews & Halcomb (2009) as quoted in Cameron (2011).

## 6 Publication of findings

One core element of academic scholarship is the inter-subjective traceability and replicability of results. Over the past years, we have witnessed a global call for more reproducible, “open science” across academic fields, including the sharing of data, materials, and measurements (for an overview, see Nosek et al. 2015, for best practice recommendations Klein et al. 2018). As a result, an increasing number of journals and policymakers adopt open research practices, such as, for example, the European Union.<sup>26</sup> Although these developments are beneficial to transparency and accountability, empirical (de-)radicalization research has some pitfalls worth considering in this context (Schumann et al. 2019). The two main issues in the publication of results are, first, about the current debate on research data management and open access of research data (Arbeitsgruppe Forschungsdaten 2018) and, second, the standards of data protection and in international and national publications. We will discuss the issues of publishing along core aspects of open science, that is (1) pre-registration (see also section 3.2), (2) research data management, and (3) public science communication

**Pre-registration.** The general idea of pre-registration is to “freeze” a final version of the theoretical background, research questions and, where applicable, hypotheses of a piece of research and fixate data collection and planned analyses before the research begins. Pre-registration is a valuable tool to avoid (unconscious) post-hoc adaption of hypotheses (harking), and to reduce analytical flexibility contributing to a low replicability of scientific findings.<sup>27</sup> Although pre-registration is mostly discussed in the context of quantitative studies and created data, pre-registration can also increase the transparency of qualitative research (Haven & van Grootel 2019). That is not to say that qualitative and quantitative pre-registration processes are identical—however, in line with our argument in the previous chapter, being explicit towards one’s own concepts, roles, biases, and aims is relevant regardless of the methodical approach. Different platforms—as the open-science framework or as [predicted.org](https://www.predicted.org/)—allow for pre-registering, including the option to keep one’s pre-registration private. As such, even when (de-)radicalization studies do not allow for full-transparency about one’s research aims (see Chapter 3 ‘Data collection’), if desired, pre-registration may be implemented in most empirical work.

**Research data management.** While (private) pre-registration of a research design is an option in some empirical approaches to (de-)radicalization research, this does not apply to empirical data itself (e.g. the open sharing of propaganda videos, case files, transcripts etc.). The background of open access in research data management originates in an attempt to avoid the duplication of data collection processes and enable a more sustainable and efficient use of collected data globally. As concerns data collection in social media networks (Facebook, Twitter) and online platforms (Youtube, Instagram, Twitch, etc.), sharing data also helps to prevent algorithmic inflation of (extremist) contents through multiplying clicks and views for data collection (see section 3.3). Sharing sanctioned data such as extremist videos, however, may be illegal and researchers might run the risk of being accused of ‘disseminating terror propaganda’. In a recent case, different EU governments requested to restrict access to the website (Wood 2018) ‘Jihadology.net’—a valuable source for academic research on Jihadi material hosted by Aron Y. Zelin (Zelin 2019). Where data is shared or published in any other way, the documentation of data sources, data production and data content was another sensitive issue. Generally, where data is shared, for reasons of transparency and accountability, details on the sources are necessary to allow for the further use of data.

In sensitive areas of research, however, as argued in Chapter 4, the documentation of the empirical field requires particular care as to data protection to avoid uncovering geolocations or incite persons to consult sanctioned online sources. Sharing anonymized “big-data” sets may also result in unintended consequences as the case of the fitness tracking app “Strava” shows, where secret American military bases became traceable by way of the jogging trails of soldiers deployed there (Hern 2018). In the case of qualitative research, the sharing of data might lead to a de-anonymization of participants with potentially severe consequences including persecution and retaliation by (former) in-group members or other actors in the field of research (Kiyak 2019, Bleich 2019).

Regardless of a project’s decision on data sharing, the question of open access research data management will become increasingly relevant for researchers and, hence, the decision for (not) sharing data, needs to be made transparent.<sup>28</sup> While there are limits to sharing sensitive data material openly in empirical (de-)radicalization research, in our experience, creating networks of trust with

26 For a summary, see <https://www.go-fair.org/2018/07/02/2351/>.

27 For more information, see <https://osf.io/prereg/>.

28 An excellent example of non-open data argumentation for a National Science Foundation grant application has recently been shared by conflict researcher and humanitarian practitioner Roxany Kristally via Twitter: <https://twitter.com/rkrystalli/status/1123205363883495424>.

other colleagues and intermediaries, or collaborations for specific projects are workable ways to increase the accessibility of data.

**Public science communication.** Although ethical challenges may arise when researchers communicate their work towards their peers and via typical research outlets, it is even more difficult for empirical (de-) radicalization research to meet the demand for public science communication (see also section 5.2). One approach is to use established networks for public science communication and acquire specific skills in communication and media training. The German National Institute for Science Communication (NaWik) provides training on public science communication and public relations offices in home institutions may offer specific training, particularly as part of academic qualification programs.

Public communication should, at all times, take into account the different ethical considerations that we emphasized in the previous chapters, for example, avoid stereotypes and carefully consider potential implications of one's statements (see also Chapter 5). In an exemplary manner, Alexandra Dick from the *Jihadism on the Internet* research group<sup>29</sup> developed an internal handout for press appearances. She stresses, amongst others, the responsibility of researchers to care for the information they provide. She depicts how this entails checking statements to ensure facticity and validity, the post-hoc request of correction in case of misleading depictions and the need for partial anonymization of persons, who are not people of public interest. From the authors' own experience, journalists are usually willing to share the broad line of questions or, in the case of TV features, the so-called 'treatment' in advance. This gives the opportunity to prepare clear, short sentences that do not require much editing by the interviewer. Researchers do, of course, have the right to refuse to comment on topics beyond their expertise and may request time to prepare their responses in recorded interviews. Both are also criteria that account for professional journalistic work following the German press codex.

To journalists, providing fact-based information is a crucial element of their work (Hanitzsch et al. 2019) that also legitimizes and strengthens their fundamental role in free societies. Good public science communication of empirical (de-)radicalization research is thus in the interest of all.

A point that connects both, research data management and public communication is that sharing and publishing data material with extremist contents is likely to contribute, in one way or the other, to reproducing the field (see section 3.3) and perpetuating extremist narratives. Giving propaganda a larger reach via public communication and referencing sources may contribute to "narrative patterns", violate copyright laws (Klonk 2019), cause further harm to survivors and shape (unintentionally) the public perception of 'problematic' content (Winter 2019). Klonk (2019) argues that potentially adverse effects may also result from screening sensitive imagery in the context of academic conferences. She suggests to exercise extreme care—or, rather, refrain from—using propaganda for mere design purposes.

Generally speaking, we encourage (de-)radicalization researchers to support transparent and accountable research via open research practices (Klein et al. 2018) in such a way that the safety of research participants is guaranteed and the risk of reproducing and perpetuating radical/extremist narratives is minimized.

## 7 Concluding remarks and practical steps

Ethics in (de-)radicalization research, as we argue in this paper, relies on a deeper professional understanding of our own roles within scholarly practice, but also on the role of academia and science in liberal democracies. It is our hope that, by systematizing the substantial experiences in research on which this paper builds, we renew and contribute to an ongoing debate on research ethics in (de-)radicalization research and beyond.

In the following, some of the main points from each chapter are summarized for ease of reference.

### Preserve and develop an ethical mindset ... ... in clarifying research context and starting the project ...

To avoid falling into the traps of contributing to securitization processes or becoming a mouthpiece of political agendas from the beginning of a research project, we have to evaluate our research topics and questions **ART**fully. As an ethical guideline for starting a project and formulation research questions, we suggest:

29 Johannes Gutenberg-University Mainz, <https://www.blogs.uni-mainz.de/fb07-ifeas-eng/jihadism-on-the-internet-images-and-videos-their-appropriation-and-dissemination/>, last accessed on November 26, 2019.



**Awareness** of the role of theory and the origins and implications of theoretical concepts;  
**Reflection** on the role you take as a researcher and keep in mind that partners and other stakeholders may follow different institutional logics and objectives  
**Transparency** about your own values, perspective, normative positions, and the emergence of your questions.

### ... in the collection of data ...

As ethical considerations in the process of data collection mostly concern the principle of ‘doing no harm’, we suggest to follow the **SAFE** guide:

**Secure** the wellbeing and safety of participants and researchers alike, for example by providing post-intervention support for participants or establishing strategies for dealing with critical incidents.  
**Avoid** unintended negative side effects of your research intervention, e.g. avoid reproducing the field and perpetuating extremist narratives by sharing data within networks of trust with other researchers or intermediaries.  
**Freedom** of research also means freedom not to conduct certain research. Carefully weigh which data is necessary for your research against the risks associated with gaining these data.  
**Explain** your research to participants a priori or ex post and be as transparent as possible to secure informed consent.

### ... in the management of data ...

Challenges of data management are tightly interlaced with legal and technical requirements. Researchers are well-advised to conduct an early assessment of possible data formats, software and hardware they need for their research and to be aware of requirements for data archiving or secure deletion. Do not hesitate to seek assistance from your legal department, data protection services and other focal points to get an overview of current legal regulations and ethical guidelines at your institution. For the archiving of data, best practices may follow the **CARE** principle:

**Cycle**: Define the data “life cycle”, including the deletion of data no longer needed, think about necessary steps to take to protect sensitive data from unauthorised access throughout the research process.  
**Anonymization**: Preserve anonymity by pseudo-anonymization/ codification—avoid quoting online sources directly.

**Regulation**: Data processing and -sharing have legal boundaries—collect? as little data as possible, but as much as necessary.

**Encryption**: If possible, get informed consent of your participants about sharing their data, establish a post-project point of contact, and, when sharing data, use encryption tools to prevent unauthorised access.

### ... in the analysis of data ...

In analysing and interpreting your data—as in all steps of the research process—**STRIVE** for excellence and professionalism. This may be guided as follows:

**Sticking** to general quality criteria of empirical research is always a good idea.  
**Remember** that your mandate as a researcher is to conduct research and that rigorous empirical research needs time. Recommendations for practice and policy are often expected but most beneficial when based on profound and solid research. Clarify your position and goals as a researcher, in particular with regard to policy recommendations.  
**Internal organization** in peer groups helps to constantly reflect your work in progress with colleagues reduces the risk of perpetuating stereotypes.  
**Validate** typologies by making sure the typologies you apply to your results are grounded in your empirical material.  
**Enable** others to evaluate the generalizability and transferability of your research results by being transparent, especially about limitations.

### ... as in the publication of findings.

The rising global call for ‘open science’ across the academic field provides some specific pitfalls in the context of empirical (de-)radicalisation research. Our advice to empirical (de)radicalisation researchers is to **SHARE** data and findings responsibly, carefully reflecting unintended side effects:

**Sharing** data is a valuable ideal to strive for. At the same time, accordant attempts should be weighed carefully against safety issues.  
**Researchers** are responsible for caring for the information they provide. When it comes to public communication they have to consider the possible implications of their statements carefully.  
**Enjoy** what you do. Please understand this paper as an offer of help to make a decision in the research process, do not get confused and enjoy what you do!



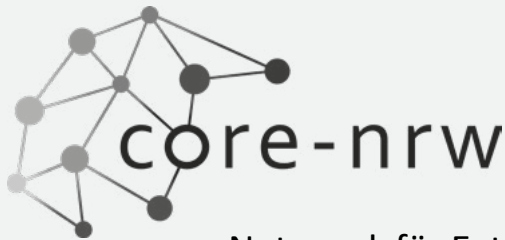
## References

- American Psychological Association (2016). Ethical principles of psychology and code of conduct. <https://www.apa.org/ethics/code/>.
- Amir-Moazami, S. (Ed.). (2018). *Der inspizierte Muslim*. Bielefeld: transcript.
- Anderson, M. B. (1999). *Do no harm*. Boulder and London: Rienner.
- Andrews, S., & Halcomb, E. (2009). *Mixed Methods Research for Nursing and Health Sciences*. London: Wiley-Blackwell: London.
- Anvari, F., & Lakens (2019). Using anchor-based methods to determine the smallest effect size of interest. <https://psyarxiv.com/syp5a/>
- Arbeitsgruppe Forschungsdaten (2018). *Research data management. A guide for researchers*. Research data working group in the priority initiative "Digital Information" of the Alliance of German Science Organisations. Potsdam: Deutsches GeoForschungsZentrum GFZ, p. 14.
- Barnes, B. R. (2018). Decolonising research methodologies: opportunity and caution. *South African Journal of Psychology*, 48 (3), 379-387. <https://doi.org/10.1177/0081246318798294>
- Bleich, H. (2019). Nichts zu verbergen. CT, July 24, 2019.
- Bloom, M., Tiflati H., & Horgan, J. (2017). Navigating ISIS's preferred platform: Telegram. *Terrorism and Political Violence* 6553: 1-13. <https://doi.org/10.1080/09546553.2017.1339695>.
- Boellstorff, T. et al. (2012). *Ethnography and virtual worlds: A handbook of method*. Princeton, Oxford: Princeton University Press.
- Borum, R. (2011). Radicalization into violent extremism II: A review of conceptual models and empirical research. *Journal of Strategic Security* 4 (4), 37-62.
- BPD & DGPS (2016). *Berufsethische Richtlinien*. [https://www.dgps.de/fileadmin/documents/Empfehlungen/berufsethische\\_richtlinien\\_dgps.pdf](https://www.dgps.de/fileadmin/documents/Empfehlungen/berufsethische_richtlinien_dgps.pdf)
- Briggle, A., & Mitcham, C. (2012). *Ethics and science: An introduction*. Cambridge applied ethics. Cambridge: Cambridge Univ. Press.
- Bröckling, U. (2008). Vorbeugen ist besser. *Zur Soziologie der Prävention*. *Behemoth. A Journal on Civilisation* 1: 38-48.
- Buchanan, E. (2017). Considering the ethics of big data research: A case of twitter and ISIS/ISIL. *PLoS ONE* 12 (12), 1-6. <https://doi.org/10.1371/journal.pone.0187155>.
- Cameron, R. (2011). *An analysis of quality criteria for qualitative research*. Central Queensland University, Gladstone, Australia cf. [https://www.anzam.org/wp-content/uploads/pdf-manager/595\\_ANZAM2011-375.PDF](https://www.anzam.org/wp-content/uploads/pdf-manager/595_ANZAM2011-375.PDF)
- Cottee, S., & Cunliffe, J. (2018). Watching ISIS: How young adults engage with official English-language ISIS videos. *Studies in Conflict and Terrorism* 0731, 1-25. <https://doi.org/10.1080/1057610X.2018.1444955>.
- Dechesne, M. (2019). Safety and security in the context of the H2020 Project DARE. Keynote at the Workshop "Ethical Questions in empirical (de-) Radicalization Research. Bridging Online and Offline." Bochum: CAIS.
- De Koning, M., Bartels, E., & Koning D. (2012). Claiming the researcher's identity: Anthropological research and politicized religion. *Fieldwork in Religion* 6(2), 168 - 186.
- Deutsche Forschungsgemeinschaft (2013). *Sicherung guter wissenschaftlicher Praxis (Safeguarding good Scientific Practice)*. Wiley-VCH Verlag. <https://doi.org/10.1002/9783527679188.oth1>.
- Deutsche Forschungsgemeinschaft & Leopoldina Nationale Akademie der Wissenschaften (2014). *Wissenschaftsfreiheit und Wissenschaftsverantwortung: Empfehlungen zum Umgang mit sicherheitsrelevanter Forschung*. [www.leopoldina.org/uploads/tx\\_leopublication/2014\\_06\\_DFG\\_Leopoldina\\_Wissenschaftsfreiheit\\_-\\_verantwortung\\_D.pdf](http://www.leopoldina.org/uploads/tx_leopublication/2014_06_DFG_Leopoldina_Wissenschaftsfreiheit_-_verantwortung_D.pdf) (Accessed October 12, 2017).
- Deutsche Gesellschaft für Soziologie (DGS) (2017). <https://soziologie.de/dgs/ethik/ethik-kodex>
- DGPuK (2017). *Ethikkodex*. [https://www.dgpuk.de/sites/default/files/Ethik-Kodex-der-DGPuK-vom-13.-Mai-2015-zuletzt-gea%CC%88ndert-am-31.-Ma%CC%88rz-2017\\_0.pdf](https://www.dgpuk.de/sites/default/files/Ethik-Kodex-der-DGPuK-vom-13.-Mai-2015-zuletzt-gea%CC%88ndert-am-31.-Ma%CC%88rz-2017_0.pdf)
- Dick, A. (2019). *Umgang mit Presseanfragen. Unveröffentlichter Leitfaden. Dschihadismus im Internet*, Johannes Gutenberg-Universität Mainz.
- Diekmann, A. (2004). *Empirische Sozialforschung. Grundlagen, Methoden, Anwendungen*. Reinbeck bei Hamburg: Rowohlt.
- Dixit, P., & Stump, J. E. (2015). *Critical methods in terrorism studies*. Abdingdon, Oxon: Routledge.
- Ebel, T., & Meyermann, A. (2015). *Hinweise zur Anonymisierung von quantitativen Daten*. *Forschungsdaten bildung informiert* Nr. 3. Frankfurt a. M.: Deutsches Institut für Internationale Pädagogische Forschung. <http://www.forschungsdaten-bildung.de/forschungsdaten-bildung-informiert>
- Ebner, J. (2017). *The Rage: The Vicious Circle of Islamist and Far-Right Extremism*. London: I. B. Tauris.
- Ess, C., & AoIR Ethics Working Committee (2002). *Ethical decision-making and Internet research: Recommendations from the AoIR Ethics Working Committee*. [www.aoir.org/reports/ethics.pdf](http://www.aoir.org/reports/ethics.pdf)
- Fielding, G., Lee, R. M., & Blank, G. (Eds.), *The SAGE Handbook of Online Research Methods* (pp.232-241). London: SAGE Publications.
- Falter, M. (2011). *Critical thinking beyond Hufeisen*. In E. Buck (Ed.), *Ordnung. Macht. Extremismus. Effekte und Alternativen des Extremismus-Modells* (pp. 85-101). Wiesbaden: VS Verlag.
- Forge, J. (2008). *The responsible scientist: A philosophical inquiry*. Pittsburgh Pa. u.a.: Univ. of Pittsburgh Press.

- Gilks, M. (2019). The security-prejudice nexus: "Islamist" terrorism and the structural logics of Islamophobia in the UK. *Critical Studies on Terrorism*. <https://doi.org/10.1080/17539153.2019.1650874>
- Goede, L.-R., Schröder, C.-P. & Lehmann, L. (2019). Perspektiven von Jugendlichen. Ergebnisse einer Befragung zu den Themen Politik, Religion und Gemeinschaft im Rahmen des Projektes „Radikalisierung im digitalen Zeitalter“ (RadigZ)“. KFN-Forschungsbericht No. 151. Hannover: KFN.
- Golla, S. J. (2019). Privacy and data protection in scientific research. Keynote at the Workshop "Ethical Questions in empirical (de-) Radicalization Research. Bridging Online and Offline" Bochum: CAIS.
- Golla, S. J., Hofmann, H., & Bäcker, M. (2018). Connecting the Dots: Sozialwissenschaftliche Forschung in Sozialen Online-Medien im Lichte von DS-GVO und BDSG-neu. *Datenschutz und Datensicherheit* (2), 89-100
- Guba E. G., & Lincoln Y. S. (2005). Paradigmatic controversies, contradictions and emerging confluences. In N. Denzin & Y. S. Lincoln (Eds.), *The Sage Handbook of Qualitative Research*, Vol. 8 (pp. 191 - 215). Thousand Oaks: Sage Publications.
- Hanitzsch, T. et al. (2019, in press). *Worlds of journalism - journalistic culture around the globe*. New York: Columbia University Press.
- Haven, T. L., & van Grootel, L. (2019). Preregistering qualitative research. *Accountability in Research* 26 (3), 1-16. <https://doi.org/10.1080/08989621.2019.1580147>.
- Hern, A. (2018). Fitness tracking App Strava gives away location of secret US Army bases. *The Guardian*, January 28, 2018.
- Hoffmann, A. et al. (2017). *Extremismus und Justizvollzug: Literatursauswertung und empirische Erhebungen. Berichte und Materialien (BM-Online)*, Band 10. Wiesbaden: Kriminologische Zentralstelle e.V.
- Hummel, K. et al. (2016). Datenlage und Herausforderungen empirischer Forschung. In J. Biene, C. Daase, J. Junk & H. Müller (Eds.), *Salafismus und Dschihadismus in Deutschland. Ursachen, Dynamiken, Handlungsempfehlungen* (pp. 43 - 77). Frankfurt a. M., New York: Campus Verlag.
- Hünler, O. (2019). Challenges and good practices for the safety and protection of researchers and participants in empirical research – the contradictions from different perspectives. In Keynote at the Workshop "Ethical Questions in empirical (de-) Radicalization Research. Bridging Online and Offline." Bochum: CAIS
- Hutchinson, J., Martin, F., & Sinpeng, A. (2017). Chasing ISIS: Network power, distributed ethics and responsible social media research. In M. Zimmer & K. Kinder-Kurlanda (Eds.), *Internet research ethics for the social age: New challenges, cases, and contexts* ( pp. 57-69). New York: Peter Lang Inc.: International Academic Publishers.
- Jukschat, N., & Leimbach, K. (2019, in press). Radikalisierung als hegemoniales Paradigma: Eine empiriebasierte kritische Bestandsaufnahme. *Behemoth – A Journal on Civilisation*.
- Kaiser, J. (2018). Laut, einflussreich und gehyped: Wie wir twitter überschätzen. *HGII Blog*, January 3, 2018. <https://www.hiig.de/hype-wie-wir-twitter-ueberschaetzen/amp/>
- Kaltmeier, O. & Berkin, S. C. (2012). *Methoden dekolonialisieren*. Münster: Westfälisches Dampfboot.
- Kämper, E. (2016). Risiken sozialwissenschaftlicher Forschung? *Forschungsethik, Datenschutz und Schutz von Persönlichkeitsrechten in den Sozial- und Verhaltenswissenschaften*. Rat für Sozial- und Wirtschaftsdaten, RatSWD Working Paper Series 255.
- Kelle, U., & Kluge, S. (2010). *Vom Einzelfall zum Typus. Fallvergleich und Fallkontrastierung in der qualitativen Sozialforschung*. 2., überarbeitete Auflage. Wiesbaden: VS Verlag für Sozialwissenschaften.
- Kiyak, M. (2019). Im Rückblick erkennt man, wie es begann. *Zeit Online*, June 19, 2019.
- Klein, O. (2018). A practical guide for transparency in psychological science. *PsyArXiv*, no. June. <https://doi.org/https://dx.doi.org/10.17605/OSF.IO/RTYGM>.
- Klonk, C. (2019). Disseminating the narrative. Keynote at the Workshop "Ethical Questions in empirical (de-) Radicalization Research. Bridging Online and Offline." Bochum: CAIS.
- Koloma Beck, T., & Werron, T. (2013). Gewaltwettbewerb. »Gewalt« in globalen Konkurrenzen um Aufmerksamkeit und Legitimität. *Leviathan*, 27, 249-277. doi:10.5771/9783845244471-247.
- Koopmans, R. (2015). Religious fundamentalism and hostility against out-groups: A comparison of Muslims and Christians in Western Europe. *Journal of Ethnic and Migration Studies*, 41:1, 33-57, DOI: 10.1080/1369183X.2014.935307.
- Kruglanski, A. et al. (2018). The making of violent extremists. *Review of General Psychology* 22 (1), 107-20. <https://doi.org/https://doi.org/10.1037/gpr0000144>.
- Law, J. (2004). *After method: Mess in social science research*. Abingdon, Oxon: Routledge.
- Logvinov, M. ( 2018). *Das Radikalisierungsparadigma. Eine analytische Sackgasse der Terrorismusbekämpfung?* Wiesbaden: Springer VS.
- Lowman, J., & Palys, T. (2001). The ethics and law of confidentiality in criminal justice research: A comparison of Canada and the U.S.. *International Criminal Justice Review* 11 (1), 1-33.
- Mahlouly, D. (2019): *Reconciling impact and ethics. An ethnography of research in violent online political extremism*. VOX-Pol Network.

- Markham, A., & Buchanan, E. (2012). AOIR guidelines: Ethical decision making and internet research version 2.0. <http://www.aoir.org/reports/ethics2.pdf>.
- Marwick, A., Blackwell, L., & Lo, K. (2016). Best practices for conducting risky research and protecting yourself from online harassment. Data & Society Guide. <https://apo.org.au/sites/default/files/resource-files/2016/10/apo-nid141976-1110461.pdf>
- McCauley, C. & Moskaleiko, S. (2008): Mechanisms of political radicalization: pathways toward terrorism. *Terrorism and Political Violence* 20: 3, 415-433.
- Meyermann, A. & Porzelt, M. (2014). Hinweise zur Anonymisierung von qualitativen Daten. *Forschungsdaten bildung informiert* Nr. 1. Frankfurt a. M.: Deutsches Institut für Internationale Pädagogische Forschung. <http://www.forschungsdaten-bildung.de/forschungsdaten-bildung-informiert>
- Mignolo, W. D., & Walsh, C. E. (2018). *On Decoloniality. Concepts, Analytics, Praxis*. Durham and London: Duke University Press.
- Moghadam, F. M. (2005). The staircase to terrorism: A psychological exploration. *American Psychologist* 60: 2, 161-169.
- Neubaum, G. (2016). Monitoring and expressing opinions on social networking sites-Empirical investigations based on the spiral of silence theory. Duisburg Essen. [https://duepublico2.uni-due.de/servlets/MCRFileNodeServlet/duepublico\\_derivate\\_00042707/Neubaum\\_Diss.pdf](https://duepublico2.uni-due.de/servlets/MCRFileNodeServlet/duepublico_derivate_00042707/Neubaum_Diss.pdf)
- Neumann, P. et al. (2018). Die Rolle des Internets und sozialer Medien für Radikalisierung und De-Radikalisierung. [https://www.hsfk.de/fileadmin/HSFK/hsfk\\_publicationen/prif1018.pdf](https://www.hsfk.de/fileadmin/HSFK/hsfk_publicationen/prif1018.pdf)
- Newman, N. et al. (2019). Reuters Institute Digital News Report 2019. <https://doi.org/10.2139/ssrn.2619576>.
- Nosek, B. A. et al. (2015). Promoting an open research culture: Author guidelines for journals could help to promote transparency, openness, and reproducibility (TOP guidelines). *Science* 348 (6242), 1422-1425. <https://doi.org/10.1126/science.aab2374>. Promoting.
- Odağ, Ö., Hofer, M., Schneider, F. M., & Knop, K. (2016). Testing measurement equivalence of eudaimonic and hedonic entertainment motivations in a cross-cultural comparison. *Journal of Intercultural Communication Research* 125 (March), 108-25. <https://doi.org/10.1080/17475759.2015.1108216>.
- Organization for Economic Co-operation and Development (OECD). (2013). The OECD Privacy Framework. [http://www.oecd.org/sti/ieconomy/oecd\\_privacy\\_framework.pdf](http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf)
- Oppenhäuser, H. (2011). Das Extremismus-Konzept und die Produktion von politischer Normalität. In E. Buck (Ed.), *Ordnung. Macht. Extremismus. Effekte und Alternativen des Extremismus-Modells* (pp. 35 - 58). Wiesbaden: Springer VS.
- Polit, D. F. & Beck C. T. (2010). Generalization in quantitative and qualitative research: Myths and strategies. *International Journal of Nursing Studies*, Volume 47, Issue 11, 2010, 1451-1458. [doi.org/10.1016/j.ijnurstu.2010.06.004](https://doi.org/10.1016/j.ijnurstu.2010.06.004)
- Przyborski, A., & Wohlrab-Sahr, M. (2008). *Qualitative Sozialforschung. Ein Arbeitsbuch*. München: Oldenbourg.
- Rieder, G., & Simon, J. (2017). Big data: A new empiricism and its epistemic and socio-political Consequences. In W. Pietsch, J. Wernecke & M. Ott (Eds.), *Berechenbarkeit der Welt? Philosophie und Wissenschaft im Zeitalter von Big Data* (pp. 85-106). Wiesbaden: Springer VS.
- Rieger, D., Frischlich, L., & Bente, G. (2013). *Propaganda 2.0: Psychological Effects of Right-Wing and Islamic Extremist Internet Videos*. Cologne, Germany: Wolters Kluwer.
- Roth, W.-M. (2005). Ethik als soziale Praxis: Einführung zur Debatte über qualitative Forschung und Ethik. *Forum Qualitative Sozialforschung / Forum: Qualitative Social Research* 6 (1).
- Salter, M., & Mutlu E. C. (Eds.). (2013). *Research methods in critical security studies*. London: Routledge. <https://doi.org/10.4324/9780203107119>
- Schaar, K. (2017). Die informierte Einwilligung als Voraussetzung für die (Nach-)nutzung von Forschungsdaten - Beitrag zur Standardisierung von Einwilligungserklärungen im Forschungsbereich unter Einbeziehung der Vorgaben der DS-GVO und Ethikvorgaben, RatSWD Working Paper, No. 264, Rat für Sozial- und Wirtschaftsdaten (RatSWD), Berlin. <http://dx.doi.org/10.17620/02671.12>
- Schiffauer, W. (2015): Sicherheitswissen und Deradikalisierung. In *Handlungsempfehlungen zur Auseinandersetzung mit islamistischem Extremismus und Islamfeindlichkeit Arbeitsergebnisse eines Expertengremiums der Friedrich-Ebert-Stiftung*, 217 - 242.
- Schumann et al. (2019). Towards open and reproducible terrorism studies. *The Data Revolution in Terrorism Research- Implications for Theory and Practice*. Oslo: Society for Terrorism Research.
- Schmidt-Kleinert, A. (2018). Ein kritischer Blick auf die Radikalisierungsforschung. Ein Es-say. *Demokratie gegen Menschenfeindlichkeit* 2, 39 - 51.
- Singelstein, T., & Stolle, P. (2012). Die Sicherheits-gesellschaft. *Soziale Kontrolle im 21. Jahrhundert*. Wiesbaden: Springer
- Smeekes, A., Verkuyten, M., & Martinovic, B. (2015). Longing for the country's good old days: National nostalgia, autochthony beliefs, and opposition to Muslim expressive rights. *British Journal of Social Psychology* 54 (3), 561-80. <https://doi.org/10.1111/bjso.12097>.
- Soeffner, H.-G. (2004). *Auslegung des Alltags – Der Alltag der Auslegung. Zur wissenssoziologischen Konzeption einer sozialwissenschaftlichen Hermeneutik*. Konstanz: UVK Verlagsgesellschaft.
- Teune, S., & Ullrich, P. (2018). Protestforschung mit politischem Auftrag? *Forschungsjournal Soziale Bewegungen* 31 (1-2), 418- 425.

- Toprak, A., & Umut A. (2019). Islamfeindlichkeit als Faktor jugendlicher Radikalisierung. *Zeitschrift für Jugendkriminalität und Jugendhilfe* 30, 20 - 25.
- Tscherwinka, R. (2014). Soziale Medien - Gegenstand und Instrument der Forschung. Rechtliche Aspekte. In C. König, M. Stahl & E. Wiegand (Eds.), *Soziale Medien: Gegenstand und Instrument der Forschung*. Schriftenreihe der ASI - Arbeitsgemeinschaft Sozialwissenschaftlicher Institute (pp. 195 –237). Wiesbaden: Springer VS..
- van Gorp, A. (2013). Research ethics in radicalisation and intervention research: How to research a sensitive topic using respondents. Utrecht.
- van Gorp, A., & Feedes, A. (2013). How to gain informed consent in radicalisation research. Amsterdam/Utrecht.
- van Zomeren, M., Postmes, T., & Spears, R. (2008). Toward an integrative social identity model of collective action: A quantitative research synthesis of three socio-psychological perspectives. *Psychological Bulletin* 134 (4), 504 -35. <https://doi.org/10.1037/0033-2909.134.4.504>.
- von Unger, H. (2014). Forschungsethik in der qualitativen Forschung: Grundsätze, Debatten und offene Fragen. In H. von Unger, P. Narimani & R. M´Bayo (Eds.), *Forschungsethik in der qualitativen Forschung: Reflexivität, Perspektiven, Positionen* (pp. 25-39). Wiesbaden: Springer VS.
- Walther, J. B, & Valkenburg, P. M. (2017). Merging mass and interpersonal communication via interactive communication technology. *Human Communication Research* 43 (4), 415 - 23. <https://doi.org/10.1111/hcre.12120>.
- Wehrheim, J. (2018). Kritik der Versicherheitlichung: Thesen zur (sozialwissenschaftlichen) Sicherheitsforschung. *Kriminologisches Journal* 03, 211-221.
- Weischenberg, S., Malik, M., & Scholl, A. (2006). Journalismus in Deutschland 2005. Zentrale Befunde der aktuellen Repräsentativbefragung deutscher Journalisten. *Media Perspektiven*, no. 7, 346 - 61.
- Wendler, D. (2017). The ethics of clinical research. *The Stanford Encyclopedia of Philosophy*. Stanford University Press. <https://plato.stanford.edu/archives/win2017/entries/clinical-research/>.
- Wendler, D., & Ried, A. (2017). In defense of a social value requirement for clinical research. *Bioethics*, 31 (2), 77-86.
- Williams, M. L., Burnap P., & Sloan, L. (2017). Towards an ethical framework for publishing twitter data in social research: Taking into account users’ views, online context and algorithmic estimation. *Sociology* 51 (6), 1149 - 68. <https://doi.org/10.1177/0038038517708140>.
- Winkler, C. (2018). Ethics is method, method is ethics: What terrorism researchers should know. *Studies in Conflict and Terrorism*, no. 2010, 1-25. <https://doi.org/10.1080/1057610X.2018.1444955>.
- Winter, C. (2019). Researching jihadist propaganda: Access, interpretation, and trauma. [https://www.resolvenet.org/system/files/2019-09/RSVE\\_RVESeries\\_ResearchingJihadistPropaganda\\_CWinter\\_May2019.pdf](https://www.resolvenet.org/system/files/2019-09/RSVE_RVESeries_ResearchingJihadistPropaganda_CWinter_May2019.pdf)
- Wood, G. (2018). Don’t shut down the internet’s biggest jihadi archive. *The Atlantic*, December 10, 2018.
- Zelin, A. Z. (2019). The case of jihadology. In *The Data Revolution in Terrorism Research: Implications for Theory and Practice*. Oslo, Norway: Society of Terrorism Research.
- Zimmer, M., & Kinder-Kurlanda, K. (2017). *Internet research ethics for the social age: New challenges, cases, and contexts*. New York: Peter Lang Inc., International Academic Publishers.



Netzwerk für Extremismusforschung  
in Nordrhein-Westfalen

CoRE – Connecting Research  
on Extremism in  
North Rhine-Westphalia

## Impressum

### Herausgeber und Kontakt

Maurice Döring

BICC · Pfarrer-Byns-Str. 1 · 53121 Bonn · Tel. +49 228.911 96-0

doering@core-nrw.de · www.core-nrw.de

Die Veröffentlichung erfolgt im Kontext des Netzwerkes CoRE-NRW, einem Verbund aus Wissenschaft und Praxis, zur Erforschung des extremistischen Salafismus und anderer Formen des Extremismus. Die Inhalte der Publikation werden allein von den Autorinnen und Autoren erstellt und verantwortet. CoRE-NRW wird vom Ministerium für Kultur und Wissenschaft des Landes NRW gefördert.

### Autorinnen

**Kerstin Eppert**, Institute for Interdisciplinary Conflict and Violence Research, Bielefeld University

**Lena Frischlich**, Institute for Communication, Westphalian Wilhelms University Muenster

**Nicole Bögelein**, Institute of Criminology, University of Cologne

**Nadine Jukschat**, Deutsches Jugendinstitut e.V.

**Melanie Reddig**, Heinrich Heine University Duesseldorf

**Anja Schmidt-Kleinert**, Department of Political Sciences, Philipps University Marburg

### Gestaltung

kipconcept gmbh, Bonn

Januar 2020

Gefördert durch

Ministerium für  
Kultur und Wissenschaft  
des Landes Nordrhein-Westfalen

