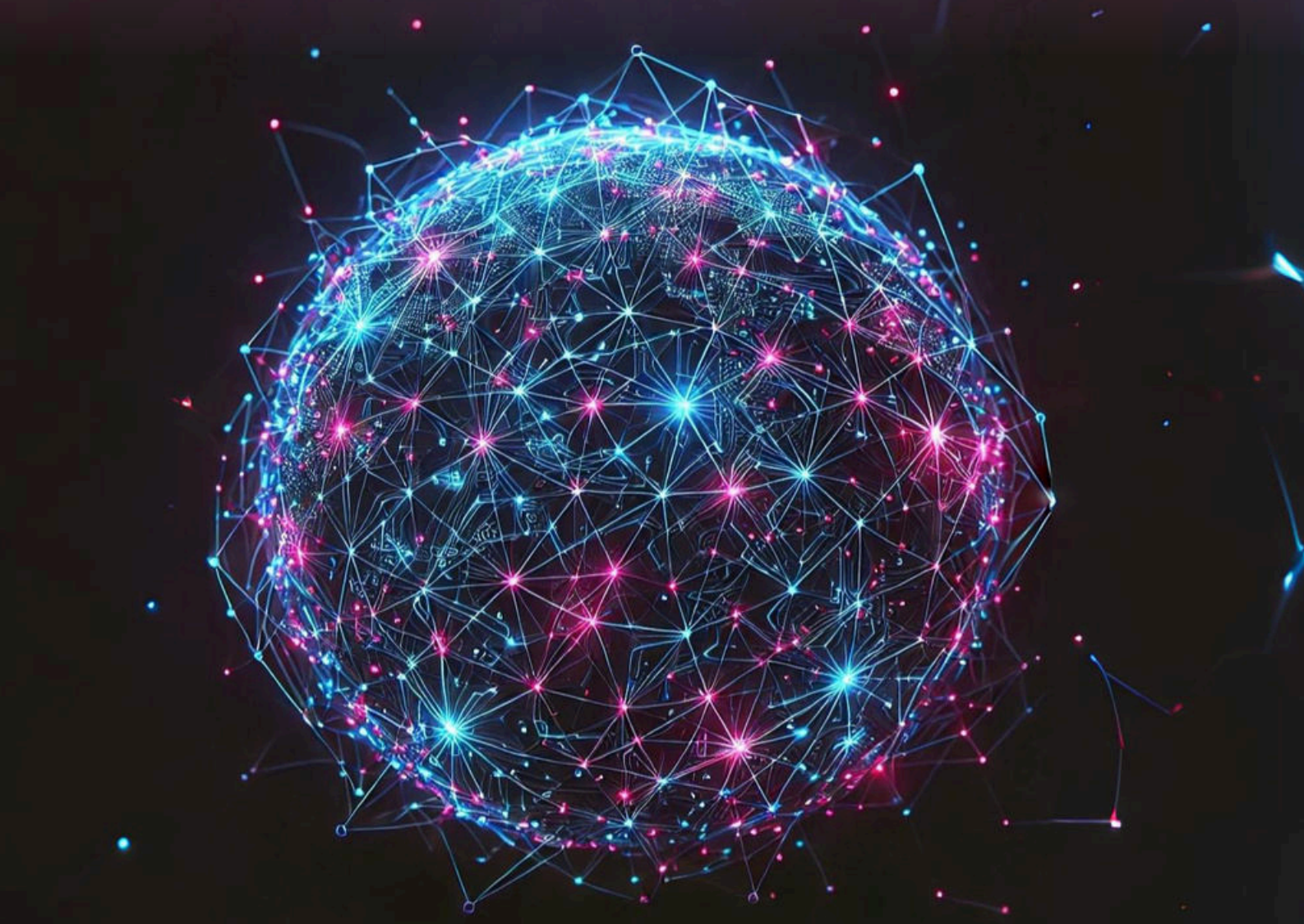
Rechtssicher und ethisch reflektiert auf Falschinformationen reagieren

Eine Handreichung für Behörden und Organisationen mit Sicherheitsaufgaben

Maria Pawelec | Michelle Duda | Luzia Sievi



Materialien zur Ethik in den Wissenschaften

Band 26

herausgegeben vom
Internationalen Zentrum für Ethik in den Wissenschaften (IZEW)
Eberhard Karls Universität Tübingen

gefördert vom
Bundesministerium für Bildung und Forschung

Diese Handreichung für Behörden und Organisationen mit Sicherheitsaufgaben entstand im Rahmen des Projekts „Trainingsansatz zur Vermittlung von Maßnahmen zur Prävention digitaler Desinformationskampagnen (PREVENT)“, gefördert vom Bundesministerium für Bildung und Forschung (2022-2025).

Alle verwendeten Illustrationen wurden mithilfe von OpenAI ChatGPT (Version o3) erstellt.

Layout von
Michelle Duda

Vorgeschlagene Zitierweise
Pawelec, Maria; Duda, Michelle; Sievi, Luzia (2025): Rechtssicher und ethisch reflektiert auf Falschinformationen reagieren. Eine Handreichung für Behörden und Organisationen mit Sicherheitsaufgaben. Tübingen: IZEW, Materialien zur Ethik in den Wissenschaften, Band 26.

ISBN: 978-3-935933-23-0

Rechtssicher und ethisch reflektiert auf Falschinformationen in den sozialen Medien reagieren

Eine Handreichung für Behörden und Organisationen mit Sicherheitsaufgaben

Maria Pawelec, Michelle Duda & Luzia Sievi

BETEILIGTE INSTITUTIONEN

Internationales Zentrum für Ethik in den Wissenschaften (Eberhard Karls Universität Tübingen)
Maria Pawelec, Luzia Sievi

Lehrstuhl für Strafrecht, Strafprozessrecht, Rechtsphilosophie und Rechtsvergleichung (Universität zu Köln)
Michelle Duda

EBERHARD KARLS UNIVERSITÄT TÜBINGEN

PREVENT

UNIVERSITÄT ZU KÖLN

Abstract

Falschinformationen können die öffentliche Sicherheit erheblich gefährden, indem sie beispielsweise in Krisensituationen Panik auslösen und die Arbeit von Einsatzkräften erschweren, aber auch indirekter indem sie das Vertrauen in staatliche Institutionen untergraben. Behörden und Organisationen mit Sicherheitsaufgaben (BOS) haben eine besondere Verantwortung, gegen Falschinformationen vorzugehen, um die Sicherheit zu wahren, müssen aber gleichzeitig Grundrechte und demokratische Werte wie die Meinungsfreiheit achten. Diese Handreichung bietet BOS daher eine fundierte, ethisch und rechtlich reflektierte Orientierung im Umgang mit Falschinformationen in den sozialen Medien. Sie basiert auf der empirischen Forschung sowie der ethischen und rechtlichen Reflexion im interdisziplinären Projekt PREVENT (2022–2025), das vom Bundesministerium für Bildung und Forschung gefördert wird. Die Handreichung enthält rechtliche Grundlagen, unter anderem zu den Themen Datenschutz und behördliche Zuständigkeiten, sowie eine systematische Übersicht möglicher Gegenmaßnahmen. Diese Maßnahmen werden ethisch sowie rechtlich bewertet. Die Handreichung vermittelt sowohl theoretische Grundlagen als auch Anregungen zur praktischen Anwendung durch Reflexionsfragen, Quizze und praktische sowie juristische Fallbeispiele. Sie dient der Sensibilisierung, Aufklärung und Information von BOS-Mitarbeitenden sowie Ehrenamtlichen im Bereich der zivilen Sicherheit. Die Handreichung ermöglicht BOS eine verantwortungsvolle Auswahl und Umsetzung von Gegenmaßnahmen im Einklang mit demokratischen, ethischen und rechtsstaatlichen Prinzipien und leistet einen wichtigen Beitrag zur Bekämpfung sicherheitsgefährdender Falschinformationen in den sozialen Medien.

Abstract (English)

False information can pose a significant threat to public safety, for example by causing panic in crisis situations and making the work of emergency services more difficult, but also more indirectly by undermining trust in state institutions. Authorities and organizations with security tasks (BOS) have a special responsibility to take action against misinformation in order to maintain security, but at the same time must respect fundamental rights and democratic values such as freedom of expression. This guide therefore provides BOS with well-founded, ethically and legally reflected guidance on how to deal with misinformation in social media. It is based on empirical research as well as ethical and legal reflection in the interdisciplinary PREVENT project (2022-2025), which is funded by the Federal Ministry of Education and Research. The handbook contains legal principles, including on the topics of data protection and official responsibilities, as well as a systematic overview of possible countermeasures. These measures are evaluated both ethically and legally. The guide provides both theoretical principles and suggestions for practical application through reflection questions, quizzes and practical and legal case studies. It serves to raise awareness, educate and inform BOS employees and volunteers in the field of civil security. The handout enables BOS responsibly select and implement countermeasures in accordance with democratic, ethical and constitutional principles and makes an important contribution to combating security-threatening misinformation in social media.

Inhaltsverzeichnis

Vorwort

Das Projekt PREVENT

PREVENT war ein interdisziplinäres Forschungsprojekt (Laufzeit 2022-2025), das vom Bundesministerium für Bildung und Forschung gefördert wurde. Ziel des Projekts war es, einen fundierten, ethisch und rechtlich reflektierten Ansatz für den Umgang mit Falschinformationen zu entwickeln – insbesondere für Behörden und Organisationen mit Sicherheitsaufgaben (BOS), die in Krisensituationen eine zentrale Rolle bei der Informationsverbreitung spielen. Das Projekt wurde von einem Konsortium getragen, dem die Universität Potsdam, die Universität Bamberg, die Universität Tübingen, die Universität zu Köln und die Virtimo AG angehörten. Die nachfolgende Handreichung wurde von Maria Pawelec und Luzia Sievi am Internationalen Zentrum für Ethik in den Wissenschaften (IZEW) der Universität Tübingen sowie von Michelle Duda vom Lehrstuhl für Strafrecht, Strafprozessrecht, Rechtsphilosophie und Rechtsvergleichung der Universität zu Köln erstellt.

Falschinformationen werden nicht nur gezielt als Desinformationskampagnen verbreitet, sondern entstehen oft auch unbeabsichtigt und haben dennoch erhebliche Auswirkungen. BOS sind potenziell stark von Falschinformationen betroffen und haben eine besondere Verantwortung, gegen diese vorzugehen (siehe Kapitel 2). Interventionen gegen Falschinformationen stehen jedoch immer auch in einem Spannungsfeld mit Grundrechten, weiteren rechtlichen Vorgaben sowie gesellschaftlichen, demokratischen und rechtsstaatlichen Werten. Nichtsdestotrotz wurden BOS als Akteure in der wissenschaftlichen und medialen Debatte um Falschinformationen bisher meist vernachlässigt.

Diese Forschungslücke ging das Projekt PREVENT an. Zunächst erarbeiteten wir im Projekt eine systematische Übersicht verschiedener möglicher Maßnahmen gegen Falschinformationen, die BOS ergreifen könnten. Auf dieser Grundlage erfolgte dann eine umfassende ethisch-rechtliche Bewertung der Maßnahmen. Diese Bewertungen haben wir in PREVENT in praxisnahen Erprobungen mit BOS validiert und weiterentwickelt, wobei deren Erfahrungen und Rückmeldungen direkt in die Evaluation und Optimierung der Maßnahmen einflossen.

Ergänzend dazu wurde im Projekt eine Social-Media-Analyse durchgeführt, um Mechanismen der Verbreitung von Falschinformationen besser zu verstehen. Zudem wurde ein Demonstrator konzipiert – ein simulationsbasiertes Tool, das die Dynamiken von Desinformationsverbreitung veranschaulicht und mögliche Gegenmaßnahmen aufzeigt.

Das Projekt PREVENT

Die ethisch-rechtliche Bewertung möglicher Maßnahmen gegen Falschinformationen in den sozialen Medien bildet das Herzstück dieser Handreichung. Sie gibt BOS bei der Auswahl von Maßnahmen Orientierung und hilft ihnen, Gegenmaßnahmen verantwortungsvoll und im Einklang mit rechtlichen sowie ethischen und demokratietheoretischen Standards auszuwählen und anzuwenden. Dabei vermittelt die Handreichung theoretisches Wissen, ermöglicht aber auch mithilfe von Quizfragen, Reflexionsfragen und Fallbeispielen eine selbstständige Überprüfung und Vertiefung.
Die vorliegende Handreichung soll somit einen entscheidenden Beitrag zu einer ethisch reflektierten und rechtssicheren Reaktion auf das drängende gesellschaftliche und sicherheitspolitische Problem der Falschinformationen leisten.

Empirische Grundlagen

Die vorliegende Handreichung basiert auf den empirischen Arbeiten der Autorinnen, einer Analyse relevanter wissenschaftlicher Literatur sowie der ethisch-demokratietheoretischen Reflexion und juristischen Analyse der Rahmenbedingungen für das Handeln von BOS und einzelner potenzieller Maßnahmen gegen Falschinformationen in den sozialen Medien.

Mitunter verweisen wir im Rahmen dieser Handreichung auf empirische Arbeiten, die im Projekt durchgeführt wurden: Zwischen April 2022 und März 2023 führten Maria Pawelec und Luzia Sievi elf semi-strukturierte qualitative Interviews mit Mitarbeitenden verschiedener deutscher BOS. Die meisten der Interviewten waren in der Öffentlichkeitsarbeit beziehungsweise den Social Media-Abteilungen ihrer Organisationen tätig. Zu den BOS gehörten u.a. Polizeibehörden auf kommunaler, Landes- sowie Bundesebene, Feuerwehren, das Technische Hilfswerk, sowie das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK). Inhalt der Interviews waren die Erfahrungen und Herausforderungen deutscher BOS mit Falschinformationen in den sozialen Medien, ihr Umgang damit, auftretende Wertkonflikte sowie mögliche Gegenmaßnahmen. Die Erkenntnisse dieser Interviews dienten der Erarbeitung einer Übersicht über mögliche Gegenmaßnahmen von BOS, deren Evaluation, und einer Rückbindung der wissenschaftlichen Arbeiten an die Praxis.

Tabelle 1: Liste der Interviewten

Interview	Organisation	Zuständigkeitsbereich	Datum
I01	Polizeibehörde einer mittelgroßen Stadt	Zwei Social Media-Manager:innen	16.05.2022
I02	Polizeibehörde einer Großstadt	Zwei Social Media-Manager:innen	28.06.2022
I03	Innenministerium eines Bundeslandes	Expert:in für Desinformation	29.03.2023
I04	Bundespolizei	Öffentlichkeitsarbeitsbeauftragte/r	01.09.2022
I05	Bundesamt für Bevölkerungsschutz und Katastrophen (BBK)	Mitarbeitende/r, die sich mit Desinformation auf strategischer Ebene befassen	29.04.2022
I06	Anonymisierte Bundes-sicherheitsbehörde	Zwei Pressesprecher:innen	17.10.2022
I07	Feuerwehr einer mittelgroßen Stadt	Zwei Social Media-Manager:innen	13.05.2022
I08	Feuerwehr einer Großstadt	Social Media-Manager:in	19.01.2023
I09	Bundesanstalt Technisches Hilfswerk (THW)	Mitarbeiter:in in der Recherche und Bearbeitung von Desinformation	26.04.2022
I10	Hilfsorganisation A	Mitarbeiter:in, die/der eine Schulung über Desinformation erstellt hat	04.04.2022
I11	Hilfsorganisation B	Pressesprecher:in	23.03.2023

Diese Ziele verfolgten des Weiteren sechs Projektworkshops, an denen weitere deutsche BOS im Rahmen des Projekts Prevent zwischen November 2022 und Juli 2024 teilnahmen. Dabei diskutierten die teilnehmenden BOS-Vertretenden u.a. mögliche Gegenmaßnahmen sowie ethische und rechtliche Überlegungen mit den Autorinnen und weiteren Projektpartnerinnen im Projekt Prevent.

Tabelle 2: Liste der Workshops

Workshop	Thema	Teilnehmende BOS	Ort	Datum
W01	Entwicklung neuer Gegenmaßnahmen für BOS	Zwei regionale Polizeibehörden	Paderborn	08.11.2022
W02	Diskussion von Rechtsfragen	Landespolizei-behörde	Köln	02.03.2023
W03	Desinformations-forschung	Eine regionale Polizeibehörde	Potsdam	28.06.2023
W04	Ethische und demokratietheoretische Bewertung von Gegenmaßnahmen	Acht BOS aus Baden-Württemberg	Stuttgart	12.10.2023
W05	Diskussion von Rechtsfragen	Eine regionale Polizeibehörde, eine staatliche Sicherheitsbehörde	Köln	14.02.2024
W06	Ethische und demokratietheoretische Bewertung von Gegenmaßnahmen	Elf BOS, überwiegend aus Baden-Württemberg	Stuttgart	18.07.2024

Weiterführende Publikationen

Im Rahmen des Projekts PREVENT entstanden zahlreiche wissenschaftliche Publikationen, die einen tieferen Einblick in zentrale Projektergebnisse bieten:

Fokus: Erfahrungen und Herausforderungen deutscher BOS mit Falschinformationen

- Pawelec, Maria; Sievi, Luzia (2023): Falschinformationen in den sozialen Medien als Herausforderung für deutsche Sicherheitsbehörden und -organisationen. In: Kriminologie – Das Online-Journal 4(5), S. 316–347.

Fokus: Ethisch-demokratietheoretische Bewertung einzelner Gegenmaßnahmen

- Sievi, Luzia; Pawelec, Maria (2025): (How) Should security authorities counter false information on social media in crises? A democracy-theoretical and ethical reflection. In: International Journal of Disaster Risk Reduction 116, S. 1-24.

Fokus: Rechtliche Bewertung einzelner Gegenmaßnahmen

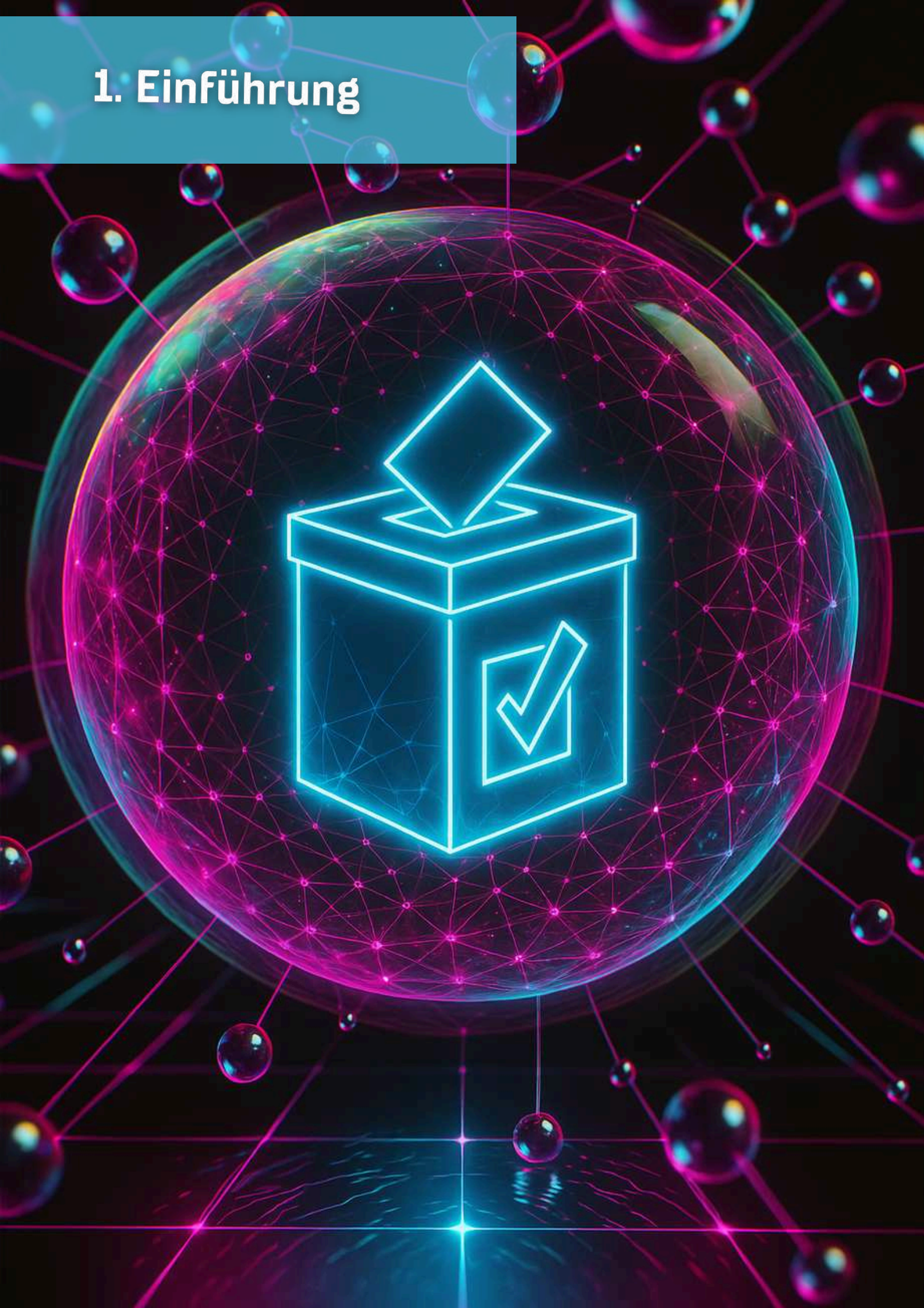
- Duda, Michelle; Evans, Alison; Rostalski, Frauke (2024): Fake News mit Social Bots bekämpfen? Zur Zulässigkeit des behördlichen Einsatzes von Social Bots im Umgang mit Falschnachrichten. In: Zeitschrift für Digitalisierung und Recht (4), S. 365-390.

Fokus: Überblick über das Projekt Prevent und (erste) Ergebnisse

- Schewina, Kai; Pawelec, Maria; Sievi, Luzia; Rieskamp, Jonas; Duda, Michelle; Hochstrate, Eric (2024): Maßnahmen zur Bekämpfung digitaler Desinformation. Interdisziplinäre Perspektiven für Sicherheitsbehörden. In: SIAK-Journal - Zeitschrift für Polizeiwissenschaft und polizeiliche Praxis (4), S. 15-29, https://www.bmi.gv.at/104/Wissenschaft_und_Forschung/SIAK-Journal/SIAK-Journal-Ausgaben/Jahrgang_2024/files/Schewina_4_2024.pdf.

- Stieglitz, Stefan; Fromm, Jennifer; Kocur, Alexander; Rostalski, Frauke; Duda, Michelle; Evans, Alison; Rieskamp, Jonas; Sievi, Luzia; Pawelec, Maria; Heesen, Jessica; Loh, Wulf; Fuchß, Christopher; Eyilmez, Kaan (2023): What Measures Can Government Institutions in Germany Take Against Digital Disinformation? A Systematic Literature Review and Ethical-Legal Discussion. Konferenzbeitrag, WI23: 18. Internationale Tagung Wirtschaftsinformatik, Paderborn.

1. Einführung



1.1 Begriffliche Grundlagen – Fake News, Desinformation, Misinformation und Falschinformationen

Fake News, Desinformation, Misinformation oder Falschinformationen – es kursieren zahlreiche Begriffe für falsche oder irreführende Informationen. Was sind die Unterschiede zwischen diesen Begriffen, wo überschneiden sie sich, und welche Begriffe beschreiben die Problematik am treffendsten? Im Folgenden wird das in dieser Handreichung verwendete Begriffsverständnis beschrieben.

Der Begriff **Fake News** wird in der Öffentlichkeit und den Medien häufig benutzt. Er bezeichnet "unechte oder gefälschte Nachrichten" (Möller et al. 2020: 11). Es ist jedoch fraglich, inwiefern falsche Informationen überhaupt als "Nachrichten" bezeichnet werden sollten. Zudem imitieren nicht alle falschen Informationen seriöse Nachrichtenformate, obwohl der Begriff eine solche Imitation zumindest anfänglich implizierte (Klicksafe 2023). Auch wurde und wird der Begriff vielfach als "Kampfbegriff" politisch instrumentalisiert, um seriöse Nachrichtenmedien zu diskreditieren (Möller et al. 2020: 11). Die Forschung zu falschen und irreführenden Informationen verwendet den Begriff "Fake News" daher selten.

Stattdessen sind in der wissenschaftlichen Auseinandersetzung die Begriffe "Desinformation" und "Misinformation" zentral. **Desinformation** bezeichnet dabei falsche oder irreführende Informationen, die absichtlich und häufig systematisch verbreitet werden. Die Intention der Verbreitenden ist dabei also entscheidend. Desinformation kann ideologischen oder ökonomischen Motiven dienen (Möller/ et al. 2020: 11). Sie wird häufig absichtlich so gestaltet, dass sie schwer zu korrigieren ist, etwa indem Fakten aus dem Kontext gerissen oder Fotos und Videos manipuliert werden (siehe Kapitel 1.8).

Im Gegensatz dazu bezeichnet **Misinformation** falsche Informationen, die unabsichtlich und im guten Glauben geteilt werden, also ehrliche Fehler, u.a. Gerüchte und Spekulationen (Möller et al. 2020: 11). Die Verbreitung von Misinformation geschieht meist unsystematisch (Möller et al. 2020: 12).

Behörden und Organisationen mit Sicherheitsaufgaben werden in ihrer täglichen Arbeit sowie in Krisen sowohl mit sicherheitsrelevanter Mis- als auch Disinformation konfrontiert. Der Begriff **Falschinformationen** dient hier als neutraler Oberbegriff für beide Phänomene.

1.2 Warum sind Falschinformationen ein Problem für BOS?

Falschinformationen bergen Risiken und Gefahren für den Einzelnen, für die BOS selbst und für die Gesellschaft: Für den Einzelnen können sie eine Bedrohung seiner Menschen- und Grundrechte, darunter seiner Sicherheit und Unversehrtheit bedeuten. So können das **Leben und die körperliche Unversehrtheit** gem. Art. 2 Abs. 2 S. 1 GG betroffen sein, wenn z.B. Desinformationen eine Massenpanik auslösen oder jemand gesundheitsgefährdend auf fehlleitende Informationen hinsichtlich Krankheiten, Wirksamkeiten von Impfstoffen oder vermeintlichen Gegenmitteln reagiert (Duda et al. 2024: 366; GG-Rixen: Art. 2 II Rn. 141 ff.). In Bezug auf die verfassungsrechtlich verbürgten Rechte kann unter anderem das **allgemeine Persönlichkeitsrecht** gem. Art. 1 Abs. 1 i. V. m. Art. 2 Abs. 1 GG tangiert sein. Dieses schützt sowohl die persönliche Ehre als auch das Recht am eigenen Wort und die informationelle Selbstbestimmung, also die personale und soziale Identität, die Selbstbestimmung, Selbstbewahrung und Selbstdarstellung (GG-Rixen: Art. 2 I Rn. 68 ff.). Diese Rechtspositionen werden beeinträchtigt durch Falschinformationen, die ehrenrührige Informationen über das Verhalten oder über Äußerungen der betroffenen Person enthalten.

BOS können direkt von Falschinformationen betroffen sein, wenn sie dadurch verleumdet und in ein schlechtes Licht gezogen werden. Dazu gehören beispielsweise Falschaussagen über das Verhalten von Beamt:innen oder über den Fokus der Arbeit von BOS und ihr Vorgehen in Krisen. Doch auch weniger gezielte Falschinformationen können die **Integrität von und das Vertrauen in BOS** erschüttern: Böswillige Akteure haben häufig zum Ziel, mit Hilfe von Desinformation wichtige gesellschaftliche Institutionen zu untergraben und das Vertrauen der Bürger:innen in sie zu zerstören (Prier 2017: 70).

Auch Polizeien, Feuerwehren und Rettungsdienste können zur Zielscheibe solcher Akteure werden. In der Folge werden nicht nur BOS selbst beeinträchtigt: Die Untergrabung von gesellschaftlichen Institutionen sowie ein fehlendes Vertrauen der Bevölkerung in Fakten untergraben **zugleich den unverfälschten Diskurs als Grundlage einer effektiven Meinungs- und Willensbildung in Demokratien sowie der Akzeptanz rechtlicher Regularien** (siehe Kapitel 1.4). Die Basis der demokratischen Legitimation des Rechtsstaats ändert sich (Duda et al. 2024: 381 ff.). Er kann seine Funktion, die verhältnismäßige Ausübung der individuellen Freiheiten der einzelnen Bürger:innen in einen Ausgleich zu bringen, von dem die freiheitliche Gesellschaft als solche profitiert, nicht mehr effektiv ausüben. Desinformationen bergen damit zugleich die Gefahr, den Rechtsstaat als solchen zu delegitimieren.

Technische Innovationen wie Entwicklungen im Bereich der generativen künstlichen Intelligenz (KI, also KI-Modelle, die darauf ausgelegt sind, neue Inhalte in Form von Texten, Bildern, Audiodateien oder Videos zu generieren) und die Ausgestaltung von sozialen Medien ermöglichen böswilligen Akteuren **neue Gestaltungs- und Verbreitungsmöglichkeiten** von Desinformationen im digitalen Raum, also von bewusst verbreiteten Falschinformationen. Ebenso ist im digitalen Raum die Gefahr gewachsen, dass sich Misinformationen, also unintendiert falsche Informationen (Müller 2024: 216) wie Gerüchte und Spekulationen verbreiten. Die sozialen Medien ermöglichen dabei eine globalisierte und schnelllebige, multilaterale Verknüpfung solcher Inhalte und erhöhen damit ihre Reichweite und ihren Einfluss, was nicht zuletzt auch durch das Geschäftsmodell der Plattformökonomie begünstigt wird (Martins Geraldes 2023: 241). Verstärkt wird dies durch verschiedene **psychologische Faktoren** (siehe Kapitel 1.5) und die Schwierigkeiten von staatlichen Institutionen, Falschinformationen (rechtzeitig) mit Gegendarstellungen zu kontern oder rechtzeitig andere wirksame Gegenmaßnahmen zu ergreifen.

Besonders in Krisenzeiten können Falschinformationen deshalb die Gesellschaft verunsichern und destabilisieren. Dies widerspricht dem Auftrag von BOS, für Sicherheit zu sorgen. Darüber hinaus können Falschinformationen auch direkter die Integrität und Legitimität, insbesondere von staatlichen, aber auch nichtstaatlichen Institutionen, untergraben.

1.3 Wertkonflikte beim Umgang mit Falschinformationen

Falschinformationen können die Sicherheit Einzelner und von Gruppen ernsthaft bedrohen. Desinformationskampagnen verfolgen zudem häufig das Ziel, demokratische Institutionen und Prozesse zu destabilisieren und auch das Vertrauen der Bevölkerung etwa in Behörden und Organisationen mit Sicherheitsaufgaben zu untergraben. In anderen Worten: Insbesondere gezielte Desinformation bedroht auch BOS selbst (Sievi/Pawelec 2025).[1] Desinformation wirkt zudem polarisierend und untergräbt die Fähigkeiten einer demokratischen Gesellschaft, faktenbasierte politische Diskussionen zu führen und entsprechende Entscheidungen zu treffen (siehe Kapitel 1.4).

Aus demokratietheoretischer Sicht sprechen jedoch auch gute Gründe dafür, dass BOS bei einer möglichen Intervention gegen Falschinformationen in den sozialen Medien vorsichtig vorgehen sollten. Denn eine solche Intervention kann wiederum selbst den **freien und ungehinderten Meinungsaustausch und die demokratische Willensbildung und Entscheidungsfindung** beeinträchtigen – insbesondere, wenn sie vonseiten staatlicher BOS erfolgt. Hier besteht "immer die Gefahr, dass der Staat seine Macht und seine Ressourcen zur Unterdrückung unpopulärer Meinungen" beziehungsweise zur Zensur nutzen und unverhältnismäßig in den Meinungsbildungsprozess eingreifen könnte (Stieglitz et al. 2023). Besonders bedeutsam ist hier, dass BOS häufig und insbesondere in Krisen und Einsätzen über einen entscheidenden Wissensvorsprung gegenüber anderen Instanzen sowie über eine besondere Autorität verfügen. Etwaige Interventionen vonseiten der BOS entfalten daher tendenziell eine größere Wirkung als beispielsweise die Posts von Einzelpersonen. Dies kann von Vorteil sein, um Falschinformationen zu korrigieren und dabei viele Menschen zu erreichen. Es bedeutet jedoch auch, dass die Social Media-Kommunikation von BOS häufig einen großen und potenziell unverhältnismäßigen Einfluss auf die öffentliche Meinungsbildung ausübt.

Auch die besondere Wahrnehmung verschiedener (insbesondere staatlicher) BOS durch Bürger:innen führt dazu, dass BOS den Meinungsbildungsprozess stets beeinflussen. Kommuniziert beispielsweise die Polizei, so "werden also regelmäßig nicht nur Ereignisse und Handlungen als gefährlich oder verboten thematisiert, sondern eben auch etwaige Handelnde als potenziell Rechtsbrechende" (Wegner et al. 2020).

1 Das vorliegende Kapitel beruht maßgeblich auf der Publikation Sievi, Luzia; Pawelec, Maria (2025): (How) Should security authorities counter false information on social media in crises? A democracy-theoretical and ethical reflection. In: International Journal of Disaster Risk Reduction 116, S. 1-24.

BOS befinden sich also in einem **Dilemma**: Auf der einen Seite müssen sie die **Sicherheit und einen funktionierenden demokratischen Meinungs- und Willensbildungsprozess sicherstellen**, indem sie unzulässige Verzerrungen durch Falschinformationen und insbesondere durch gezielte Desinformation eindämmen. Auf der anderen Seite dürfen sie nicht unverhältnismäßig in diese Prozesse eingreifen und dabei insbesondere das Recht der Bürger:innen auf freie Meinungsäußerung und Information einschränken.

BOS müssen sich daher an das **Neutralitätsgebot** und die "Verpflichtung zur (politischen) Mäßigung" halten (Wegner et al. 2020). Doch auch wenn BOS versuchen, bei der Reaktion auf Falschinformationen neutral zu handeln, werden BOS-Mitarbeitende stets durch ihre eigenen sowie durch organisationsinterne Werte, Kulturen und Vorprägungen beeinflusst und sind niemals gänzlich neutral (siehe Kapitel 9.2). **BOS sollten jedoch versuchen, die negativen Auswirkungen ihrer Eingriffe in den Meinungsbildungsprozess so gering wie möglich zu halten**. Dabei müssen sie in Hinblick auf die Menschenrechte und die Werte liberaler Demokratien keineswegs neutral sein. Sie sollten bei Reaktionen auf Falschinformationen jedoch stets reflektieren, ob sie beispielsweise bestimmte Bevölkerungsgruppen diskriminieren. Auch sollten BOS so objektiv wie möglich berichten und ihre Quellen offenlegen (Sievi/Pawelec 2025).

Insgesamt bestehen jedoch beim Umgang mit Falschinformationen unauflösbare **Wertkonflikte**, u.a. zwischen Sicherheit und Meinungsfreiheit, Schutz und Autonomie, Privatsphäre und Transparenz (Sievi/Pawelec 2025). Den richtigen Umgang mit solchen Wertkonflikten müssen BOS-Mitarbeitende im Einzelfall abwägen.

Dabei gilt aus ethischer Sicht: Je schwerwiegender und unmittelbarer eine konkrete Bedrohung ist, desto stärker können Eingriffe in bestimmte Rechte gerechtfertigt sein, um Maßnahmen zur Minimierung der Bedrohung zu ermöglichen. So wäre es problematisch, wenn BOS bei einem Terroranschlag falsche Informationen über den Standort, die Anzahl oder die Ziele der Täter:innen in den sozialen Medien unwidersprochen kursieren ließen, da dies beispielsweise zu unnötigen Fluchthandlungen oder auch Anfeindungen führen könnte und damit eine schwerwiegende Sicherheitsgefährdung darstellen würde. Umgekehrt wäre es in Hinblick auf die Meinungsfreiheit aber auch problematisch, wenn staatliche Behörden solche Diskussionen nach dem Anschlag zensierten, wenn sie keine Sicherheitsrelevanz mehr haben (Sievi/Pawelec 2025).

1.4 Der unverfälschte Diskurs und die demokratische Gesellschaft

Übergreifend gefährden Falschinformationen eine funktionierende Gesellschaft insofern, als sie den **rationalen Diskurs in der Bevölkerung** beeinflussen. Dies wirkt sich nicht zuletzt auch auf deren Akzeptanz von staatlichen Regularien aus (Duda et al. 2024: 366). Für eine funktionierende Gesellschaft ist es nämlich notwendig, dass zwischen Bevölkerung und Staat eine Verständigung stattfindet, die auf eine echte Teilnahme der Bevölkerung am rationalen Diskurs gerichtet ist. Wenn die Bevölkerung das Vertrauen in die Richtigkeit des Rechts verliert, schwächt dies die **Loyalität gegenüber dem Rechtssystem** enorm.

Ein unverfälschter und freier Diskurs ist jedoch nicht nur für die Akzeptanz von rechtlichen Regularien zentral, sondern auch für eine funktionierende **demokratische Meinungs- und Willensbildung**. Nur wenn Bürger:innen ihre Meinungen frei kundtun, austauschen und debattieren können, können sie zu tragfähigen, akzeptierten und legitimen Lösungen für gesellschaftliche Probleme kommen. Die Kommunikation innerhalb eines öffentlichen Raums muss also durch “das freie Prozessieren von Themen und Beiträgen, Informationen und Gründen“ (Habermas 1994: 138 f.) möglich sein. Demokratien werden somit also auch durch den freien und offenen Diskurs als Legitimationsbasis charakterisiert und legitimiert. Gerade diese Offenheit macht sie **angreifbar**: Desinformationen bedrohen diesen freien und unverfälschten Diskurs, denn sie bergen unter anderem das Risiko von **Silencing Effekten**, bei denen andere durch Falschinformationen in ihrer freien Meinungskundgabe eingeschüchtert werden (Rostalski 2024: 63), etwa dadurch, dass Fehlvorstellungen oder diskriminierende Vorurteile über andere Menschen verstärkt werden. Darüber hinaus führen sie zu einer Unsicherheit in der Bevölkerung darüber, was wahr ist, und erschweren dadurch eine sinnvolle politische Meinungsfindung.

Anders gesagt: Die Sachverhalte und Tatsachen, auf die sich die Meinungsbildung und -äußerung in der Bevölkerung beziehen, werden als Fundament einer wehrhaften Demokratie entzogen. Desinformationen wirken sich somit schädlich auf öffentliche Debatten aus. Gleichzeitig können jedoch auch Maßnahmen zu ihrer Bekämpfung (darunter auch solche, die von BOS ergriffen werden) in die freie Meinungsäußerung eingreifen und zu Silencing-Effekten führen.

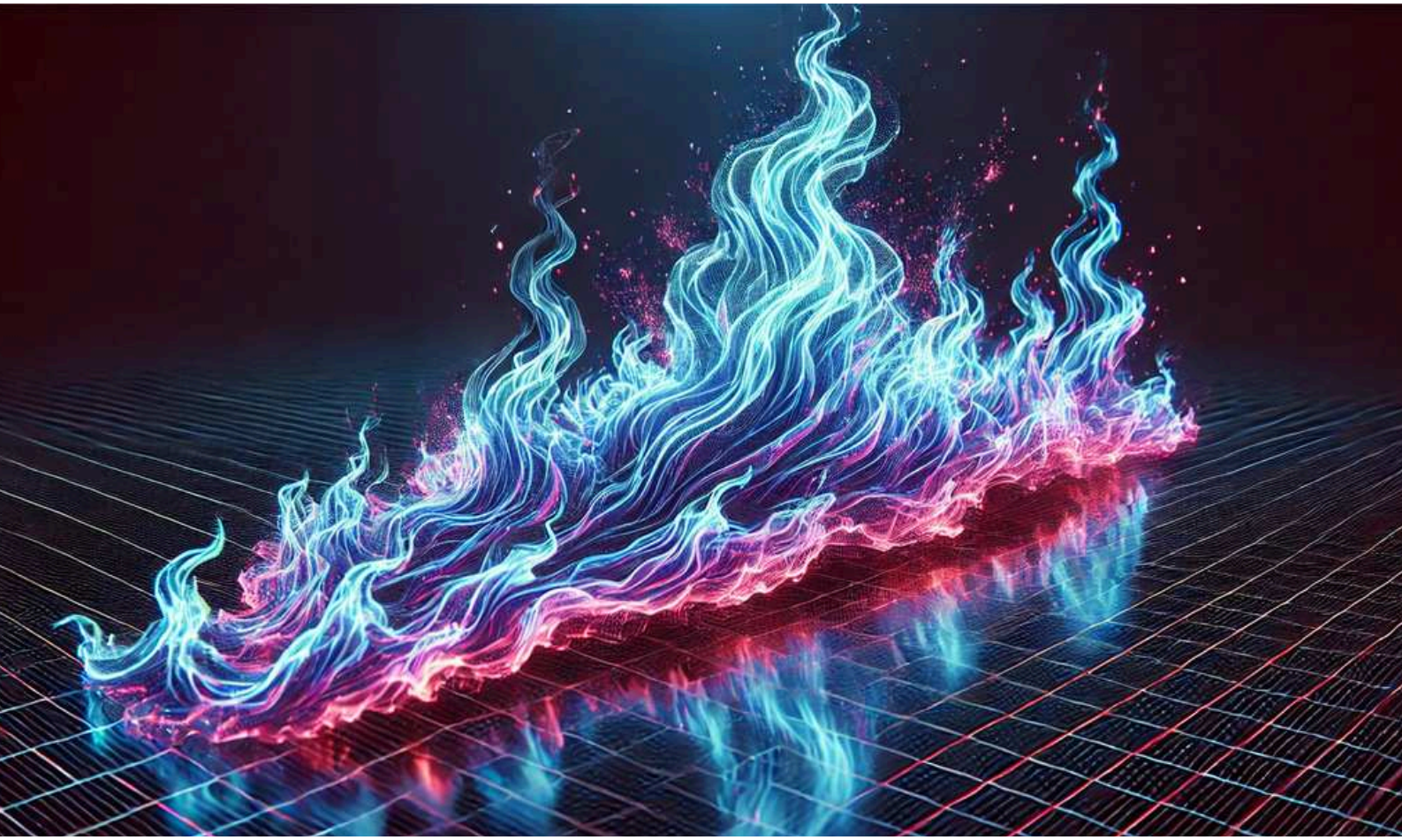
1.5 Digitalisierung und psychologische Faktoren als Brandbeschleuniger

Falschinformationen sind kein neuartiges Phänomen. Die diversen Möglichkeiten der digitalen Verbreitung machen das Problem jedoch drängender denn je. Die Gesellschaft ist nun durch digitale Technologien global vernetzt, wodurch Falschinformationen eine besonders **hohe Reichweite** erhalten. Sie können in **Sekundenschnelle** unter anderem über soziale Medien verbreitet werden. Darüber hinaus ermöglichen **technische Innovationen** auf der Basis von KI neue Formen der Bild-, Video- und Tonmanipulation (bspw. sog. "Deep Fakes"; siehe Kapitel 1.8), eine neue Quantität der Generierung von textbasierten Desinformationen sowie eine zusätzliche Erhöhung der Reichweite aufgrund neuartiger Verbreitungsformen wie den Einsatz von Social Bots (Norri-Sederholm et al. 2023: 266).

Auch undurchsichtige **Empfehlungsalgorithmen** tragen zu dieser Problematik bei. Sie beeinflussen, welche Inhalte die meiste Aufmerksamkeit erhalten (Thieltges und Hegelich 2017: 504). Diese begünstigen zusätzlich soziale Phänomene wie Filterblasen oder Echokammern. Filterblasen entstehen durch eine von Empfehlungsalgorithmen vorgenommene Vorsortierung und Personalisierung von Inhalten. Dadurch werden Nutzenden hauptsächlich solche Inhalte zur Verfügung gestellt, die ihren (politischen) Einstellungen entsprechen, dadurch allerdings das Risiko bergen, dass Offenheit gegenüber abweichenden Positionen schwindet. Echokammern wiederum beschreiben den Effekt, dass Nutzende digitaler Medien dazu tendieren, verstärkt den Kontakt zu Personen und Institutionen zu suchen, die ihre eigene Meinung teilen und entsprechend Mitgliedern der eigenen sozialen Gruppe gegenüber bereits positiver und vertrauensvoller eingestellt sind. Externen Informationen wird weniger Glauben geschenkt. Die Existenz von Filterblasen und Echokammern ist nicht unumstritten, wird in der wissenschaftlichen Literatur aber anhaltend diskutiert (Welzenbach-Vogel 2021: 187 ff.).

Konsens herrscht dabei weitgehend darüber, dass Menschen dazu neigen, Informationen (und auch Falschinformationen) eher zu glauben (und auch zu verbreiten), wenn sie ihren eigenen Überzeugungen entsprechen. Dieses Phänomen wird "confirmation bias" genannt (Prier 2017: 57).

Empfehlungsalgorithmen machen sich solche psychologischen Inklinationen zu Nutze, um die Verweildauer der Nutzenden auf der eigenen Plattform und damit auch die gesammelten Daten zu maximieren, welche wiederum die Grundlage für den ökonomischen Erfolg der Plattformen bilden. In anderen Worten: Menschen tendieren dazu, länger mit negativen oder stark emotionalisierenden Inhalten zu interagieren und diese eher zu teilen. Dies ist für die Plattformbetreiber von Vorteil, da ihr ökonomisches Modell auf der Sammlung möglichst vieler Daten über die Nutzenden basiert, und sie mehr Daten sammeln können, je länger und je mehr Menschen auf ihren Plattformen interagieren (**Aufmerksamkeitsökonomie, Plattformkapitalismus**). Das Geschäftsmodell der sozialen Medien begünstigt somit die Verbreitung von Falschinformationen.



1.6 Sollten BOS auf (bestimmte) Falschinformationen reagieren?

Beim Umgang mit Falschinformationen begegnen BOS regelmäßig unauflösbaren Wertkonflikten (siehe Kapitel 1.3).[2] Sie müssen ihre Reaktionen daher stets im Einzelfall abwägen. Dabei können und sollten sie sich einige Fragen stellen, um zu einer ethisch möglichst reflektierten Reaktion zu gelangen.

Die erste Frage ist, **wer entscheidet, was "wahr" ist** und was eine Falschinformation darstellt. Dies ist nicht immer einfach, da faktische Aussagen häufig mit Meinungen vermischt werden, insbesondere bei politisch oder emotional aufgeladenen Themen. Auch falsche Äußerungen können dabei Meinungselemente enthalten. Akteure, die gezielt Desinformation streuen, reißen zudem häufig Fakten, die an sich nicht falsch sind, aus dem Kontext, berichten lückenhaft, oder säen Zweifel. Solche Aussagen können BOS häufig nicht eindeutig als falsch kennzeichnen. Die Unterscheidung zwischen falschen und richtigen Aussagen ist daher anspruchsvoll, aber auch politisch. BOS müssen sich daher fragen, ob ihre Mitarbeitenden geschult sind, um Falschinformationen von legitimen Meinungsäußerungen in einer pluralistischen Gesellschaft zu unterscheiden. Zudem: Reflektieren sie kritisch, wie ihre eigenen möglichen Vorurteile, politischen Meinungen oder die Kultur ihrer Institutionen ihre Entscheidungen beeinflussen können?

Im nächsten Schritt müssen BOS entscheiden, ob sie auf eine bestimmte Falschinformation **reagieren oder nicht**. Dazu ist zunächst die Frage der rechtlichen Zuständigkeit zentral (siehe Kapitel 4). BOS müssen dann aus ethischer Sicht prüfen, ob die Falschinformation eine Bedrohung der Sicherheit Einzelner, der Demokratie oder Institutionen wie der BOS selbst darstellt, ob sie also geeignet ist, das Vertrauen in BOS so weit zu untergraben, dass ihre Funktionsfähigkeit und Aufgabenerfüllung beeinträchtigt werden.

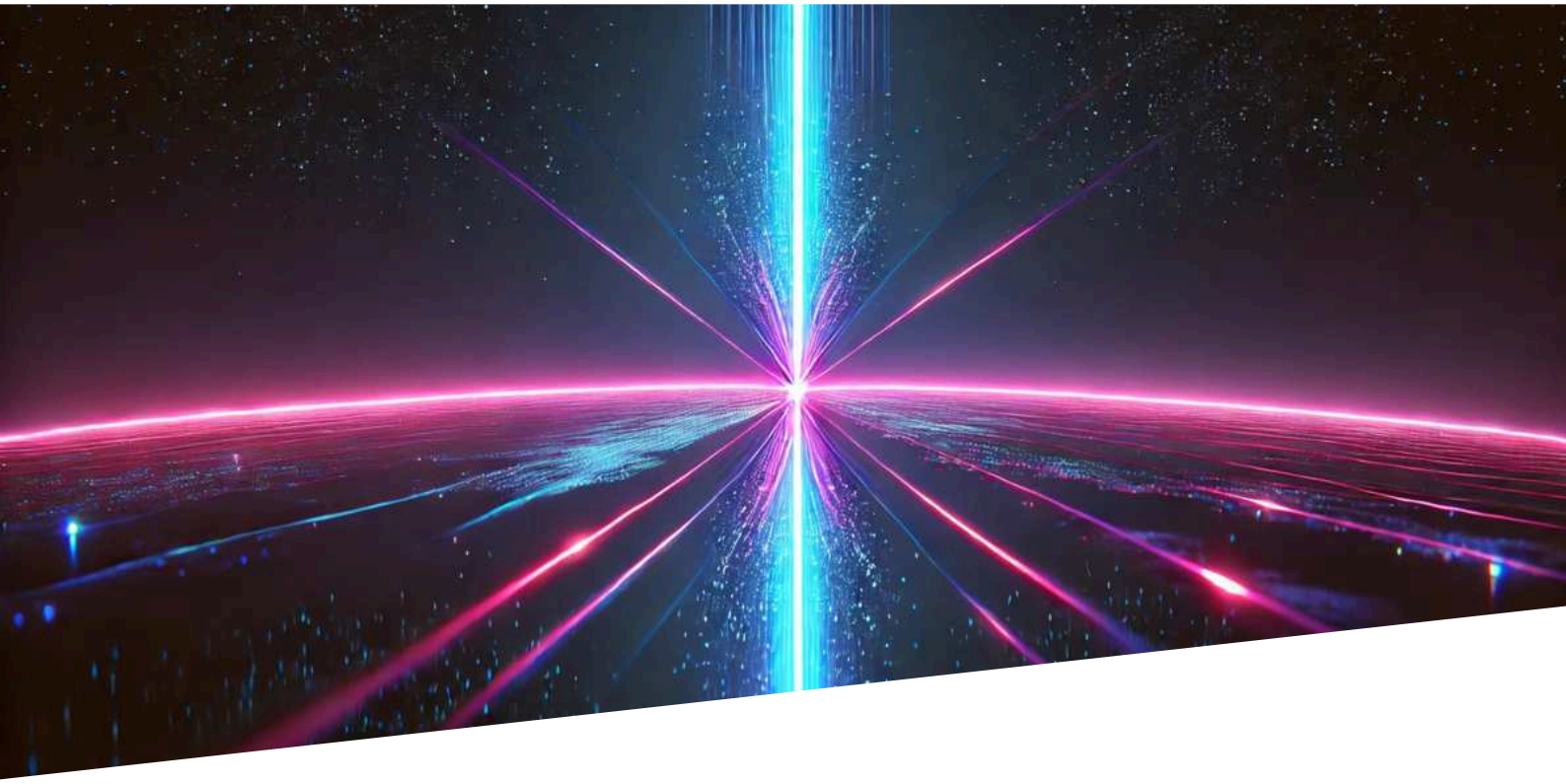
2 Das vorliegende Kapitel beruht maßgeblich auf der Publikation Sievi, Luzia; Pawelec, Maria (2025): (How) Should security authorities counter false information on social media in crises? A democracy-theoretical and ethical reflection. In: International Journal of Disaster Risk Reduction 116, S. 1-24.

Auch die Reichweite der Falschinformation spielt bei der Gefährdungsbeurteilung eine Rolle (siehe Kapitel 8). Wenn eine Falschinformation nur eine geringe Bedrohung für die Sicherheit darstellt und mögliche Gegenmaßnahmen relativ stark in die Meinungsfreiheit eingreifen würden, kann es angemessener sein, nicht (wieder) tätig zu werden. Eine funktionierende, deliberative Demokratie sollte in der Lage sein, einigen falschen oder irreführenden Aussagen zu widerstehen. Zudem kann eine Reaktion durch BOS einer falschen Information auch unfreiwillig mehr Reichweite verschaffen. Zu bedenken ist hierbei, dass wissenschaftliche Studien zeigen, dass die Veröffentlichung von Gegeninformationen die ursprüngliche Falschinformation in den Köpfen der Lesenden verstärken kann, weil sie die Falschinformation vertrauter machen und entsprechende Assoziationen stärken.

Wenn es für BOS angemessen ist, überhaupt auf eine Falschinformation zu reagieren, müssen sie sich **für eine oder mehrere Gegenmaßnahmen entscheiden**. Diese müssen verhältnismäßig im Hinblick auf die Bedrohung durch die Falschinformation sein. Bei einer Gefährdung von Leib und Leben ist ein intensiverer Eingriff in die freie Meinungsäußerung legitimer als bei weniger gefährlichen Falschinformationen. Gegenmaßnahmen müssen zudem mit den Zielen der BOS übereinstimmen, wobei BOS auch unintendierte Nebenfolgen berücksichtigen müssen. BOS sollten also beispielsweise bedenken, ob sie durch eine Reaktion einer Falschinformation eine größere Reichweite verschaffen und damit die Sicherheitsgefährdung gegenüber einer Situation verstärken, in der sie nicht reagieren. Sie müssen beispielsweise auch abwägen, ob bestimmte Maßnahmen wie Nudging (siehe Kapitel 7) als paternalistisch wahrgenommen werden, das Vertrauen in der Bevölkerung in sie schwächen und daher ihrem Ziel entgegenstehen, als vertrauenswürdige Anlaufstelle für Informationen in Krise zu fungieren. Hier sind somit auch Wertkonflikte bei der Umsetzung der Maßnahmen zentral. Auf diese Wertkonflikte gehen die vorliegende Handreichung je Maßnahme gesondert ein.

Um in rechtlicher Hinsicht das Grundrecht der Meinungsfreiheit hinreichend beachten zu können, müssen BOS beim Umgang mit Falschinformationen auf Social Media immer zwischen der **Meinungsfreiheit und gegenüberstehenden Rechten** wie den Persönlichkeitsrechten der betroffenen Personen oder der Gefahr für die Allgemeinheit **abwägen** (detailliert hierzu siehe Kapitel 3). Äußerungen, die lediglich Werturteile darstellen, sind grundsätzlich durch die Meinungsfreiheit geschützt, selbst wenn sie provokativ oder unangemessen sind. Schwierig wird es jedoch, wenn eine Äußerung falsche Tatsachenbehauptungen enthält, die erwiesen oder bewusst falsch sind. In solchen Fällen muss die Meinungsfreiheit zugunsten des Schutzes ihr gegenüberstehender, schützenswerter Rechte zurücktreten. Hierbei ist es wichtig, dass BOS den Kontext und den Wahrheitsgehalt der Aussagen prüfen. Sollte es sich um ernsthafte Falschinformationen handeln, die das Vertrauen in die Behörde oder ihre Funktion beeinträchtigen, kann die Behörde auch rechtliche Schritte wie Strafanzeigen oder Unterlassungsansprüche einleiten. So stellt die Behörde sicher, dass ihre Aufgabe im öffentlichen Interesse weiterhin erfüllt werden kann.

Es kommt also stets auf den Einzelfall an, ob und wie BOS auf bestimmte Falschinformationen in den sozialen Medien reagieren sollten. Die vorliegenden Materialien sollen BOS dabei unterstützen, ethisch und rechtlich angemessene Gegenmaßnahmen zu wählen.



1.7 Inwiefern betreffen Falschinformationen die Gefahrenabwehr?

Die **Gefahrenabwehr** umschreibt die (polizeiliche) Aufgabe, von Einzelnen und dem Gemeinwesen Gefahren abzuwehren, welche die öffentliche Sicherheit oder Ordnung bedrohen, und Störungen der öffentlichen Sicherheit oder Ordnung zu beseitigen, soweit es im öffentlichen Interesse geboten ist. Bei Falschinformationen liegt der Fokus auf der Bedrohung der öffentlichen Sicherheit. Öffentliche Sicherheit umfasst den Schutz der Unverletzlichkeit der objektiven Rechtsordnung, den Schutz der subjektiven Rechte und Rechtsgüter der/des Einzelnen sowie den Schutz des Bestandes des Staates und sonstiger Träger der öffentlichen Gewalt, ihrer Einrichtungen und Veranstaltungen. Innerhalb der rechtlichen Gefahrenabwehr wird dieser Begriff verwendet, um den Rahmen für den Schutz vor Gefährdungen zu definieren, die das friedliche Zusammenleben der Gesellschaft sowie die Funktionsfähigkeit des Staates und seiner Institutionen gefährden können (Münch/Kunig-Kunig/Berger, Art. 13 Rn. 76 ff.).

Falschinformationen bedrohen die öffentliche Sicherheit auf mehreren Ebenen. Ihre Verbreitung kann die **Unverletzlichkeit der objektiven Rechtsordnung** sowie potenziell **den Schutz der subjektiven Rechte und Rechtsgüter des Einzelnen** betreffen. Unzutreffende oder manipulierte Darstellungen von rechtlichen Rahmenbedingungen oder Handlungen von Behörden können das Vertrauen der Bevölkerung in die Rechtsordnung und in die Verlässlichkeit staatlicher Institutionen schwächen (Martins Geraldes 2023: 245). Falsche oder irreführende Informationen können Einzelpersonen in ihrer Würde, Freiheit oder Sicherheit beeinträchtigen. Beispielsweise können unrichtige Darstellungen von Personen oder Gruppen in den Medien zu Rufschädigungen, Diskriminierung oder gar zu körperlichen Gefährdungen führen. In solchen Fällen sind die subjektiven Rechte der betroffenen Einzelpersonen direkt bedroht, was eine Verletzung ihrer Grundrechte darstellen kann (Ueberschär 2021: 114 ff.). Medizinische Falschinformationen oder Panik infolge von Falschinformationen können zudem die Grundrechte auf Leben und körperliche Unversehrtheit betreffen.

Verletzungen subjektiver Rechte können zugleich die objektive Rechtsordnung verletzen, wenn das “geschriebene Recht” sie erfasst. Eine Verletzung des persönlichen Ehre etwa kann zugleich zur Folge haben, dass die verbreitende Person zugleich den Tatbestand einer Verleumdung gem. § 187 StGB erfüllt. Ebenso gefährden Falschinformationen den **Schutz des Bestandes des Staates und seiner Einrichtungen und Veranstaltungen**. Falschmeldungen über eine Naturkatastrophe, eine Terrorgefahr oder eine gesundheitliche Krise können etwa die Reaktionsfähigkeit und -qualität der staatlichen Institutionen und Sicherheitsbehörden beeinträchtigen.

Die Behörden könnten durch eine falsche Gefahreneinschätzung Ressourcen auf eine nicht bestehende Bedrohung lenken oder anderweitig benötigte Ressourcen aufwenden, um der Falschinformation zu begegnen, was die Handlungsfähigkeit der staatlichen Strukturen einschränkt und somit den Bestand des Staates gefährdet. Ein besonders relevanter Aspekt im Bereich der Falschinformationen sind Wahlen. Werden diese durch Falschinformationen beeinträchtigt, kann dies nicht nur im Sinne einer Gefährdung staatlicher Veranstaltungen unter die Gefahrenabwehr fallen. Konsequent betrachtet kann eine Beeinträchtigung demokratischer Wahlen durch Falschinformationen auch die Parlamente und die Regierungen betreffen, sei es in ihrer Zusammensetzung oder in ihrer allgemeinen Funktionsfähigkeit, wenn aufgrund der erkannten Beeinflussung durch Falschinformationen etwa die Wahlen wiederholt werden müssten.

1.8 Fokus: Deepfakes

Deepfakes sind manipulierte oder synthetisch erstellte audio-visuelle Medien (also Bilder, Audiospuren und Videos) menschlicher Gesichter, Körper oder Stimmen, die zumeist mit Hilfe von KI erstellt wurden. Deepfakes zeigen somit, wie Menschen Dinge tun oder sagen, die sie nie getan oder gesagt haben.

Die Qualität und Zugänglichkeit der Technologie ist in den letzten Jahren rasant gestiegen. Mit Hilfe von Bild-, Audio- und zunehmend auch Videogeneratoren ist es nun auch technischen Lai:innen möglich, in kürzester Zeit ohne technisches Know-How überzeugende mediale Fälschungen zu erstellen. Deepfakes sind somit ein mächtiges neues Werkzeug für Akteure, die gezielt Desinformation verbreiten wollen. Gleichzeitig können jedoch auch viele legitime Nutzungen von Deepfakes, etwa für Satire und Parodien, verunsichern und manipulativ wirken.

Wenn Sie mehr über die Technologie hinter Deepfakes und konkrete Anwendungsfälle lernen möchten, finden Sie hier eine interaktive Lerneinheit, die von Studierenden der Medienwissenschaften der Universität Tübingen mit Unterstützung von Maria Pawelec, wissenschaftlicher Mitarbeiterin am Internationalen Zentrum für Ethik in den Wissenschaften (IZEW) erstellt wurde: https://view.genially.com/65a27a299ca9090014cf0a93

Weiterführende Informationen zum Thema Deepfakes finden Sie im Dossier der Bundeszentrale für politische Bildung “Wenn der Schein trügt – Deepfakes und die politische Realität”: https://www.bpb.de/lernen/bewegtbild-und-politische-bildung/551578/wenn-der-schein-truegt-deepfakes-und-die-politische-realitaet/

Spielen Sie “Fake it to Make it”

Fake It
To Make It

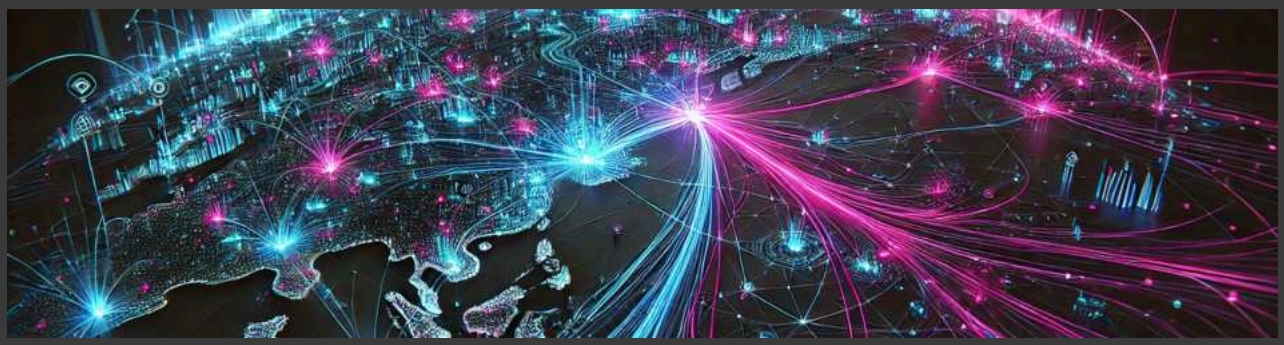
“Fake it to Make it” erlaubt es Ihnen, in die Rolle eines Akteurs zu schlüpfen, der gezielt Desinformation verbreiten möchte, um ein bestimmtes finanzielles Ziel zu erreichen. Sie lernen in diesem Spiel viel darüber, wie Desinformation gestaltet wird, um besonders wirkmächtig und reichweitenstark zu sein. Der Schwerpunkt liegt auf politischer Desinformation: https://fakeittomakeit.de/

Amoklauf in München 2016

Am 22. Juli 2016 erschoss ein rechtsradikal motivierter 18-jähriger neun Menschen im Olympia-Einkaufszentrum (OEZ) München und verletzte fünf weitere. Kurz nach dem ersten Notruf an die Polizei gab es bereits Tweets zum Geschehen; allein in der Nacht wurden über 200.000 Tweets zum Amoklauf abgesetzt. Dazu gehörten verschiedene Gerüchte wie die Mutmaßung, dass es mehr als eine/n Täter:in gäbe, und dass an mehreren Orten in München Schüsse gefallen seien. Ein Fernsehsender verbreitete ein Bild einer Schießerei in Südafrika, im Glauben, dass es sich um ein Bild aus München handele. Augenzeugen filmten und streamen live vom Ort des Geschehens, was Gerüchte und Spekulationen weiter anheizte. Diese führten unter anderem dazu, dass Menschen von Orten flüchteten, an denen gar keine Gefahr für sie bestand. Dabei kam es zu zahlreichen Verletzungen. So sprangen Menschen beispielsweise durch die Scheiben des Münchner Hofbräuhauses.

Der Amoklauf in München 2016 gilt als Weckruf für deutsche BOS in Hinblick auf die Bedeutung der sozialen Medien und von Falschinformationen in Krisen, sowie der Reaktion der Behörden auf diese Falschinformationen: Das Social Media Team der Münchner Polizei reagierte schnell auf die Flut an Tweets und kommunizierte noch während des Anschlags und in der Nacht aktiv über Twitter. Sie informierte in 113 Tweets auf Deutsch, Englisch und Französisch über die Lage, “informierte, warnte, stellte richtig, beruhigte und ermahnte gelegentlich, dass manche Bilder und Videos eher dem Täter helfen könnten.” (Möser 2020: 212–213). Durch diese aktive Kommunikation “dominierte” (ebd.) sie schließlich die Informationslage auf Twitter; ihre Tweets wurden etwa 100 Millionen Mal gesehen. Die besonnene und präsente Reaktion der Münchner Polizei galt als bedeutsam, um die Falschinformationen und die Angst in der Bevölkerung in den Griff zu bekommen. Der Leiter der Pressestelle Marcus da Gloria Martins wurde für diese Kommunikation im September 2016 vom Bundesverband deutscher Pressesprecher ausgezeichnet.

Flut im Ahrtal 2021



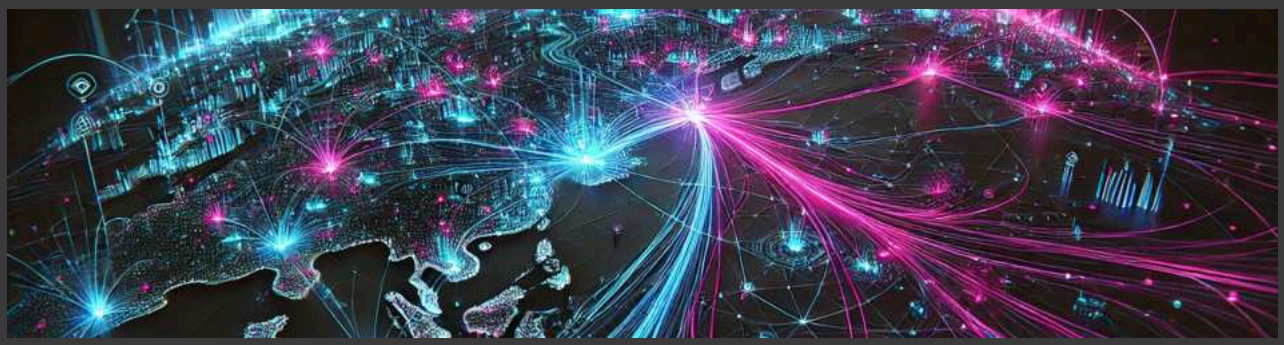
Im Juli 2021 verursachten schwere Niederschläge in Deutschland und anderen Ländern in West- und Mitteleuropa extreme Hochwasser. In Deutschland starben mindestens 188 Menschen; besonders betroffen waren die Bundesländer Nordrhein-Westfalen und Rheinland-Pfalz und insbesondere das Ahrtal.

Im Zuge des Hochwassers kursierten zahlreiche Gerüchte und Spekulationen, teils aber auch bewusst verbreitete Desinformation. Zu ersteren gehörten Gerüchte in den sozialen Medien, die Steinbachtalsperre, eine Talsperre in Nordrhein-Westfalen, sei gebrochen oder werde dies bald tun. Die Talsperre war durch das Hochwasser extrem belastet; unter anderem half das THW mit, sie durch Abpumpen zu entlasten. Das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe hatte entsprechend bereits simuliert, wozu ein Bruch der Talsperre führen würde. Die Talsperre hielt jedoch. Dennoch führten Gerüchte über ihren (bevorstehenden) Bruch dazu, dass Menschen nachts aus ihren Häusern flohen.

Als Reaktion entsandte die Bundespolizei einen Hubschrauber, um die Sperre nachts zu überwachen. Die Feuerwehr in Flerzheim im westlichen Rhein-Sieg-Kreis fuhr durch bedrohte Orte und sagte per Lautsprecher durch, dass es keine Evakuierungen gebe und der Damm halte. Die Feuerwehr Euskirchen veröffentlichte auf Facebook ein Bild der intakten Talsperre mit dem Text: „Aufgrund der Falschmeldung, der Damm der #Steinbachtalsperre wäre gebrochen, hat ein Hubschrauber der #Bundespolizei den Damm überflogen und keine Risse festgestellt!“. Am nächsten Tag folgte eine offizielle Entwarnung.

Auf Facebook kursierten während der Hochwasserlage zudem Fotos, die zeigten, wie sich Einsatzkräfte am Nürburgring sammelten. Dabei wurde fälschlicherweise behauptet, dass die Einsatzkräfte hier von ihrer Arbeit abgehalten würden. Mehrere beteiligte Organisationen wie das Technische Hilfswerk und die Bundeswehr stellten daraufhin in den sozialen Medien klar, dass der Nürburgring lediglich als Sammelstelle für die Einsatzkräfte genutzt wurde.

Flut im Ahrtal 2021



Teilweise wurde auch bewusst Desinformation geteilt. So verbreiteten Menschen per Megaphon aus Fahrzeugen, die polizeilichen Einsatzfahrzeugen ähnelten, die falsche Botschaft, dass die Zahl der Einsatzkräfte im Katastrophengebiet reduziert worden sei. Interessant ist daran, dass diese Desinformation "analog" und nicht hauptsächlich in den sozialen Medien gestreut wurde. Anders war dies bei der drastischen Desinformation, im Ahrtal seien 600 Kinderleichen aufgetaucht. Diese basierte auf einem kurzen Ausschnitt eines frühen TV-Berichts eines Reporters, in dem dieser jedoch keine entsprechenden Zahlen genannt, sondern nur von einzelnen Funden gesprochen hatte. Der Clip wurde extrem gekürzt geteilt und schnell mit Verschwörungserzählungen der QAnon-Bewegung verbunden. Demnach unternehme eine Elite geheime, tödliche Experimente an Kindern; deren Leichen seien nun durch das Hochwasser zutage befördert worden. Diese Desinformation wurde auch international geteilt, ohne dass dafür je Beweise geliefert wurden. Entsprechend stellte das Polizeipräsidium Koblenz klar, dass es zu keinem solchen Fund gekommen war.

Im Kontext des Hochwassers 2021 in Deutschland kursierten somit zahlreiche Misinformationen in der verunsicherten Bevölkerung. Akteure verbreiteten jedoch auch bewusst ideologisch motivierte Desinformation, die teils mit internationalen Verschwörungserzählungen verbunden wurde. Das Ziel solcher Desinformation ist häufig die Destabilisierung demokratischer Institutionen wie staatlicher (Sicherheits-)Behörden sowie das Untergraben des Sicherheitsgefühls der Menschen. Ganz praktisch behinderten Mis- und Desinformation im Einsatz während des Hochwassers häufig die Arbeit der Einsatzkräfte, verängstigten die Betroffenen und banden Ressourcen, die anderweitig benötigt wurden.

Linksammlung Wissenswertes zu Falschinformation

CORRECTIV ist eine unabhängige Plattform für investigativen Journalismus, die regelmäßig Faktenchecks, aber auch Hintergrundmaterialien z.B. zur Medienbildung veröffentlicht: https://correctiv.org/

Mimikama e.V. ist ein Verein zur Aufklärung über Falschinformationen und, nach eigener Aussage, "Internetmissbrauch". Die Webseite des Vereins bietet eine Plattform für deutschsprachige unabhängige Faktenchecks aktueller (Falsch-)Informationen ebenso wie wichtige Hintergrundinformationen, darunter ein Glossar wichtiger Begriffe sowie eine Sammlung von Quizzes zum Thema Falschinformationen: https://www.mimikama.org/

Faktenchecks bietet darüber hinaus das Angebot **tagesschau Faktenfinder**: https://www.tagesschau.de/faktenfinder

2015 legte die EU vor dem Hintergrund russischer Desinformation und Propagandaaktivitäten den Grundstein für eine Einheit zur Bekämpfung von Desinformation beim Europäischen Auswärtigen Dienst, **"EUvsDisinfo"**. Die Webseite der Einheit bietet in englischer (sowie russischer und ukrainischer) Sprache interessante Hintergrundinformationen über Desinformation mit einem Schwerpunkt auf ausländischer Einflussnahme und hybrider Kriegsführung: https://euvsdisinfo.eu/learn/

Die **Deutsche Presse-Agentur (dpa)** bietet eine eigenständige Faktencheck-Redaktion, die gezielt mögliche Falschbehauptungen überprüft und professionelle Faktenchecks erstellt. Sie führt einen Faktencheck-"Newsletter", in dem sie über aktuelle Faktenchekcs berichtet, bietet ein Faktencheck Trainingsprogramm an und kooperiert mit diversen digitalen Plattformen wie TikTok, WhatsApp und Facebook: https://www.dpa.com/de/faktencheck

GADMO (German-Austrian Digital Media Observatory) ist der größte Zusammenschluss von Faktencheck-Organisationen und Forschungsteams aus Deutschland und Österreich im deutschsprachigen Raum, der sich zum Ziel gesetzt hat, Desinformationskampagnen zu identifizieren und Faktenchecks bereitzustellen. Nach Themen aufgeteilt kann man aktuelle Faktenchecks verfolgen: https://gadmo.eu/

Linksammlung Wissenswertes zu Falschinformation

Das **EFCSN (European Fact-Checking Standards Network)** vertritt die Interessen europäischer Faktenprüfer:innen, die sich für die Einhaltung und Förderung hoher Standards in der Faktenprüfung und Medienkompetenz einsetzen, um Falschinformationen im öffentlichen Interesse zu bekämpfen. Der EFCSN und seine verifizierten Mitglieder bekennen sich zu den Prinzipien der Meinungsfreiheit. Sie fördern den Zugang der Öffentlichkeit zu überprüften und verlässlichen Informationen und bieten Bildungsangebote, um die Fähigkeit der Menschen zu stärken, die Richtigkeit von Informationen im öffentlichen Raum zu bewerten: https://efcsn.com/

Auch die **Bundesregierung** hat auf ihrer Website eine Übersicht angelegt, mit welcher sie darlegt, woran man Desinformationen erkennen kann: https://www.bundesregierung.de/breg-de/aktuelles/desinformation-erkennen-1750146

2. Sollten BOS auf (bestimmte) Falschinformationen reagieren?

2.1 Ethisch-rechtliche Abwägungen zu Falschinformationen

Falschinformationen bergen für Einzelne und die Gesellschaft gravierende Gefahren (siehe Kapitel 1.2). Daher scheint es gerechtfertigt, dass BOS bei der Bekämpfung von Falschinformationen tätig werden und Gegenmaßnahmen ergreifen. Doch reicht der Hinweis auf die Gefahren in jedem einzelnen Fall aus? Kann damit jede beliebige Maßnahme gerechtfertigt werden? Nein, denn auch wenn im Allgemeinen die Gefahren von Falschinformationen hoch sind, müssen BOS dennoch **den Einzelfall betrachten und eine ethische, praktische sowie rechtliche Abwägung treffen**, ob und welche Reaktion auf eine Falschinformation gerechtfertigt ist.

Was gilt es aus praktischer, rechtlicher und ethischer Sicht abzuwägen? Bei der Frage, ob BOS auf Falschinformationen reagieren sollen, steht die **öffentliche Sicherheit im Konflikt mit anderen Werten**, die in unserer Gesellschaft ebenfalls von hohem Rang sind. Unter öffentlicher Sicherheit verstehen wir den Schutz der objektiven Rechtsordnung im Sinne der Gesamtheit des geschriebenen Rechts, der subjektiven Rechte und Rechtsgüter Einzelner und des Bestandes des Staates und seiner Einrichtungen. Der Schutz der objektiven Rechtsordnung bedeutet, dass (drohende) Verletzungen geschriebenen Rechts, wie etwa die Körperverletzungstatbestände im Strafrecht, möglichst verhindert werden sollen.

Der Schutz dieser Sicherheit kann im Widerspruch stehen zur Wahrung von **Grundrechten, nämlich der Meinungs- und Informationsfreiheit, der freien Entfaltung der Persönlichkeit (Autonomie) und das Gleichheitsgrundrecht** (auch im Sinne einer Diskriminierungsfreiheit). Ebenfalls zentral sind wichtige Werte wie die **Privatheit** einzelner Bürger:innen und der **Datenschutz**, die **Neutralität** von Sicherheitsbehörden und die **Sachlichkeit und Richtigkeit** von ihnen geteilter Informationen, aber auch die **Gerechtigkeit**.

Die Problematik ist nämlich, dass **Maßnahmen gegen Falschinformationen ihrerseits negative Wirkungen** entfalten können. Blockt beispielsweise ein Social Media Team eine Nutzerin, weil diese wiederholt sicherheitsgefährdende Aussagen auf einem Kanal der Feuerwehr postet, so erhöht es zwar die Sicherheit der anderen Follower:innen, schränkt aber eben auch die Meinungsfreiheit dieser Nutzerin ein. Die Abwägung, die also getroffen werden muss, ist, ob die Sicherheit in diesem Fall höher zu gewichten ist als die Meinungsfreiheit. Ein anderes Beispiel ist, dass die Polizei nicht immer Falschinformationen zu Todesfällen oder Verletzungen von Personen korrigieren kann, wenn sie etwa die Persönlichkeitsrechte wie die Ehre, Selbstbestimmung oder Privatsphäre der betroffenen Personen bewahren muss (siehe Kapitel 9.3).

Solche Abwägungen können nicht pauschal getroffen werden. In manchen Fällen ist die Gefahr durch eine Falschinformation für viele Menschen so gravierend, dass es ethisch unverantwortlich wäre, wenn Sicherheitsbehörden nicht reagieren würden. Es wäre beispielsweise höchst problematisch, wenn im Falle eines terroristischen Anschlages falsche Informationen über den Ort des Angriffs, die Anzahl der Angreifenden oder deren Ziele unkommentiert von den Behörden auf Social Media kursieren könnten. Darüber hinaus sind BOS rechtlich verpflichtet, Gefahren für die öffentliche Sicherheit abzuwehren und Schaden von der Bevölkerung abzuwenden. Eine unterlassene Reaktion könnte nicht nur das Vertrauen in staatliche Institutionen gefährden, sondern auch gegen bestehende gesetzliche Handlungspflichten verstoßen (siehe Kapitel 1.7). Hier ist die **Sicherheitsgefahr so groß, dass die Meinungs- und Informationsfreiheit dagegen nachrangig sind**. Denn wenn die Informationen dazu beitragen, dass die Menschen unsichere Orte aufsuchen oder in Panik geraten, dann könnte deren Leib und Leben (d.h. die körperliche Unversehrtheit) bedroht sein. Es wäre aber wohl ebenso rechtlich unzulässig, wenn die Behörden solche Diskussionen nach der Attacke, wenn keine Gefahren oder Sicherheitsbedenken mehr bestehen, unterbinden würden. In einem solchen Fall stehen der Meinungs- und Informationsfreiheit gerade keine gewichtigen Sicherheitsinteressen gegenüber (Hong 2022: 141 f.; Schlömer und Kehrberg 2025: 5).

2.2 Was wollen wir bewahren?

Die dahinterliegende und **grundlegende Frage** bei diesen Abwägungen ist: **In welcher Gesellschaft wollen wir leben?** Die Antwort, die sich unsere demokratische Gesellschaft in Deutschland selbst gegeben hat, ist, dass wir natürlich einerseits in einer sicheren und einer funktionierenden Gesellschaft leben wollen, aber dass uns ebenso unsere demokratischen Freiheiten und Menschenrechte am Herzen liegen. Spezifischer können wir die Frage in Bezug auf Falschinformationen formulieren: **Was wollen wir bewahren**, das von Falschinformationen bedroht ist? Und was wollen wir bewahren, wenn wir gegen Falschinformationen vorgehen?

Wie schon im Kapitel 1.2 “Warum sind Falschinformationen ein Problem?“ aufgeführt, können Falschinformationen nicht nur die **Sicherheit, sondern auch die demokratische Willensbildung bedrohen**, indem sie das Vertrauen in demokratische Institutionen untergraben und die Gesellschaft spalten. Sicherheit, eine funktionierende Demokratie und unsere Grund- und Menschenrechte wollen wir schützen. Doch leider können auch Gegenmaßnahmen von BOS schädlich für den **freien Meinungsaustausch und die demokratische Willensbildung**, die Ausübung weiterer **grundrechtlich geschützter Positionen und den Bestand des Rechtsstaats, die Autonomie und Privatheit der Bürger:innen, die Gerechtigkeit und Diskriminierungsfreiheit, sowie den Datenschutz** sein. Mit guten Gründen gibt es Abwehrrechte gegen den Staat. In Bezug auf die Meinungsfreiheit sichern sie, dass staatliche Organe nicht den freien Meinungsaustausch und die politische Willensbildung der Bürger:innen beeinflussen, dominieren oder gar zensieren. Ein übermächtiger Staat, der seinen Bürger:innen bestimmte Meinungen aufdrängt und ihm nicht genehme Meinungen unterdrückt, ist nicht demokratisch oder rechtsstaatlich. Daher ist den Polizeien, Feuerwehren und Rettungsdiensten ihre eigene **Neutralität, Sachlichkeit und Richtigkeit** so wichtig (W04). Diese tragen ebenfalls dazu bei, die hohen Güter der Meinungs- und Informationsfreiheit zu bewahren, indem sie verschiedene Meinungen und Lebensweisen respektieren und staatliche Propaganda vermieden wird. Doch auch die genannten anderen Grundrechte und Werte (Persönlichkeitsrechte, Gleichheit, Datenschutz, Gerechtigkeit) können durch Gegenmaßnahmen von BOS bedroht werden. Auf die **jeweiligen ethischen und rechtlichen Abwägungen gehen wir in den einzelnen Kapiteln zu den möglichen Gegenmaßnahmen** (Kapitel 6) näher ein.

Darüber hinaus haben wir allgemeine Fragen zusammengetragen, die Ihnen bei der ethischen und rechtlichen Abwägung, ob BOS auf bestimmte Falschinformationen reagieren sollten, helfen können.

BOS müssen also immer wieder neu fragen, welche wichtigen Werte, Grundrechte und sonstige Rechtspositionen eine spezifische Falschinformation bedroht und welche anderen Werte BOS selbst bedrohen, wenn sie auf diese Falschinformation reagieren. Die folgenden Fragen können Ihnen hierbei als Ausgangspunkt dienen, um eine ethische, rechtliche und praktische Abwägung zu treffen, ob Sie überhaupt auf spezifische Falschinformationen reagieren sollten oder nicht, und falls ja, mit welchen Mitteln und in welchem Umfang.

1. Ist Ihre Behörde oder Institution überhaupt in einem bestimmten Fall zuständig?

Es kann wichtig sein, diese Frage vorab zu klären. Wir geben hierzu mehr rechtliche Hintergründe und ausführliche Informationen im Kapitel “Zuständigkeiten”.

2. Ist die problematische Passage eine Meinungsäußerung, die zu tolerieren ist?

Diese Frage kann im Einzelfall sehr schwierig zu beantworten sein, denn gerade desinformierende Akteure mischen oft wahre und falsche Aussagen mit Meinungsäußerungen. Ausführlich behandeln wir diese Problematik im Kapitel “Wie unterscheide ich Falschinformationen von Meinungsäußerungen?”

3. Stellen Falschinformationen überhaupt eine Gefahr dar?

Nicht alle Falschinformationen sind auch sicherheitsrelevant. Wenn beispielsweise ein Youtuber veröffentlicht, Schleswig-Holstein habe die Rechtschreibung an Schulen abgeschafft und Lehrkräfte würden keine Fehler mehr zählen (Scherndl 28.05.2024), so ist das zwar falsch, aber nicht sicherheitsrelevant – zumindest, solange diese Desinformation nicht zu gewaltsamen Protesten führt, bei denen etwa die körperliche Unversehrtheit Einzelner konkret bedroht wäre.

Für eine rechtliche und ethische Abwägung gilt: **Je weniger die Sicherheit und grundrechtlich geschützte Positionen von Menschen bedroht werden, desto höher sind die Meinungs- und Informationsfreiheit, die menschliche Autonomie, die Persönlichkeitsrechte und der Datenschutz zu gewichten**. Eine Falschinformation, die keine oder eine sehr geringe Gefahr für die genannten Werte, Interessen und Rechtspositionen darstellt, benötigt nicht unbedingt eine Reaktion. Jedenfalls beeinflusst dies die Anforderungen an Intensität, Umfang und Wahl der Maßnahme. In solchen Fällen mag es auch reichen, dass der freie Meinungsaustausch zwischen den Menschen dazu führt, dass die Aussage mittels Kommunikation (siehe hierzu Kapitel 9.) widerlegt wird. In solchen Fällen kann ein demokratischer Staat seinen Bürger:innen auch im Rahmen ihrer Selbstbestimmung und Autonomie zugestehen, sich eine eigene Haltung zu veröffentlichten Falschinformationen zu bilden. Ebenfalls bestünde dann kein Grund, wieso der Datenschutz und die Persönlichkeitsrechte von Menschen ausgesetzt werden sollten.

Falls Sie zu dem Schluss kommen, dass es in manchen Fällen auch ohne eine nennenswerte Sicherheitsbedrohung dennoch gute andere Gründe gibt, wieso von Behörden eingegriffen werden muss, sollte die Wahl der Gegenmaßnahmen auf jene Maßnahmen fallen, die den freien Meinungsaustausch möglichst wenig beeinträchtigen und möglichst wenig weitere demokratische Rechte beschneiden. Die **Intensität der Maßnahme sollte also proportional zum erwartbaren Schaden** durch die Falschinformation ausfallen (Grundsatz der Verhältnismäßigkeit).

4. Ist die Reichweite der Falschinformation so groß, dass sie vielen Menschen schadet?

In die Bewertung, wie hoch der potenzielle Schaden durch eine Falschinformation sein könnte, müssen auch ihre **Reichweite, die Sensibilität des Themas** – etwa, wenn ein Thema sehr intim ist, oder vulnerable Gruppen bedroht – und die **zeitliche Dringlichkeit** einfließen. Bei einer geringen Reichweite sind nur wenige Menschen betroffen und die Gefahr durch die Falschinformation damit potenziell gering. Dies ist beispielsweise der Fall, wenn eine Falschinformation von einem Account mit sehr wenigen Follower:innen verbreitet und entsprechend nicht weiter aufgegriffen wird. In einem solchen Fall müssen BOS – wie in Frage 3 ausgeführt – abwägen, ob die Sicherheitsbedrohung überhaupt Eingriffe in andere Rechte rechtfertigt.

Es ist jedoch möglich, dass die gefährliche Falschinformation **in der Zukunft den Sprung in reichweitenstärkere Verbreitungskanäle** schaffen kann. Eventuell könnte es BOS mit einer schnellen Gegenmaßnahme gelingen, eine Falschnachricht im Keim zu ersticken, bevor sie eine größere Verbreitung findet (W04). In einem solchem Fall muss abgewogen werden, wie wahrscheinlich es ist, dass die Nachricht in Zukunft eine größere Reichweite erreicht und damit Schaden anrichtet, und ob deswegen Gegenmaßnahmen angebracht sind.

Zudem sollten BOS berücksichtigen, dass sie **potenziell selbst dazu beitragen, die Reichweite einer Falschnachricht zu erhöhen**. Wenn sie öffentlich über eine eher unbekannte Falschnachricht aufklären, hören mitunter erst dadurch viele Menschen davon (I02, I05). Studien zeigen, dass Falschnachrichten den Menschen im Gedächtnis bleiben, selbst wenn sie von der Widerlegung wissen (z.B. Lewandowsky et al. 2012). Auch Widerlegungen können daher dazu beitragen, dass Falschinformationen Verbreitung finden (ausführlicher siehe hier das Kapitel 9).

5. Welche Maßnahme sollten BOS in welchem spezifischen Fall anwenden?

Verschiedene Maßnahmen setzen an verschiedenen Stellschrauben an und haben verschiedene Wirkungen. In den nachfolgenden Kapitel erläutern wir ausführlich die möglichen Erfolge und möglichen negativen Wirkungen verschiedener Maßnahmen, so dass BOS passgenauer entscheiden können, welche Maßnahme sie anwenden wollen.

6. Wer entscheidet wie, ob eine Information vertrauenswürdig oder falsch ist?

In manchen Fällen ist es für BOS-Mitarbeitende einfach zu recherchieren, ob eine Information richtig oder falsch ist, insbesondere, wenn sie als Polizeien oder Feuerwehren einen schnellen Zugang zu Katastrophenorten haben. Dann können sie beispielsweise selbst nachprüfen, ob bei Flutkatastrophen ein Damm gebrochen ist oder nicht, ob es bei einer Katastrophe Tote gab, oder wissen Bescheid, ob Einsatzkräfte abgezogen worden sind oder nicht.

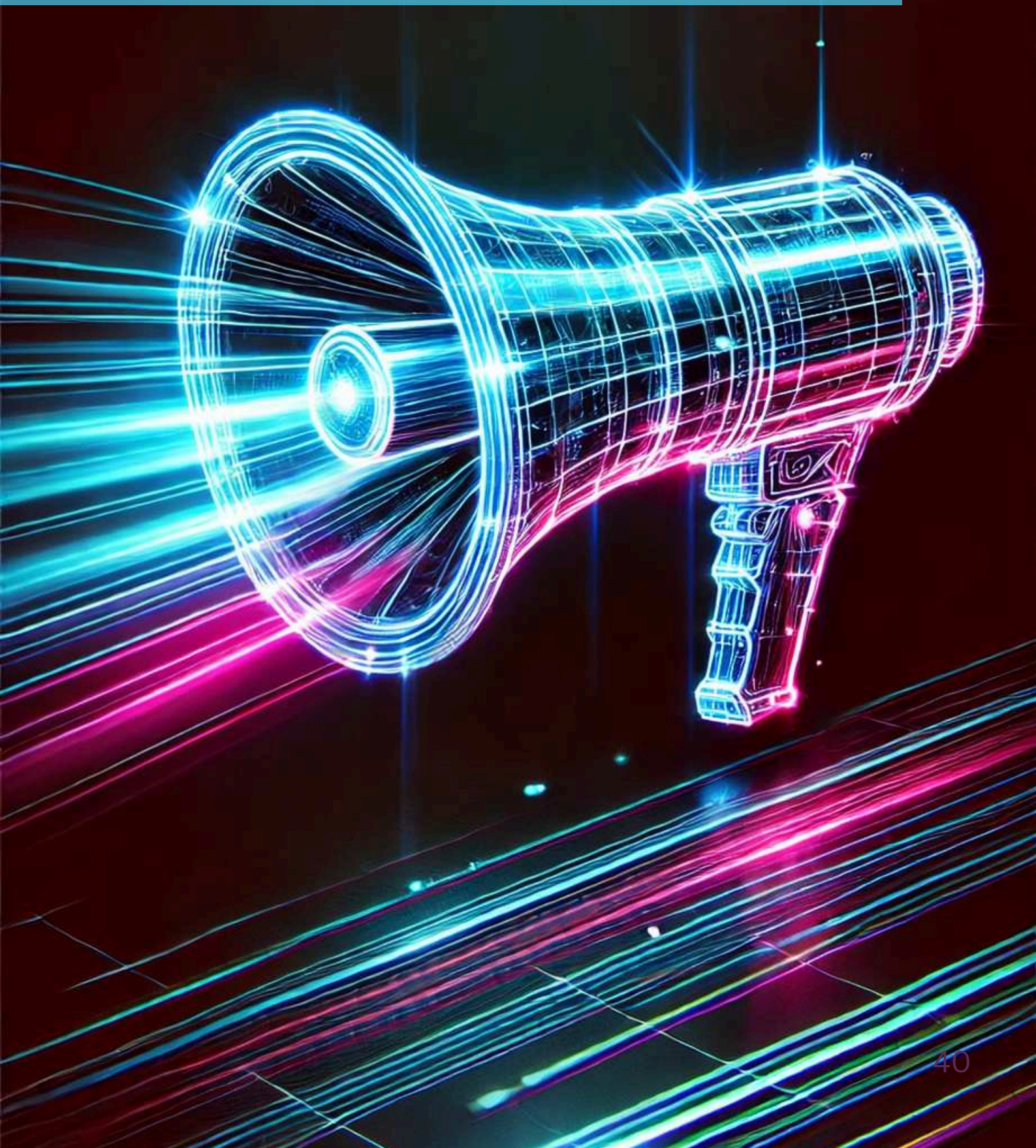
Doch gerade in der Coronakrise zeigte sich, dass auch Behörden **nicht immer rechtzeitig einen gesicherten Wissensstand** haben. Gerade zu Beginn der Pandemie gab es große Unsicherheiten darüber, wie wirkungsvoll Masken sind, später gab es Unsicherheiten in Bezug auf die Gefahren und Wirksamkeiten von Impfungen.

Es ist eine **Strategie desinformierender Akteure, solche Unsicherheiten auszunutzen**, zu verstärken und damit die Gesellschaft zu spalten. Gerade in Krisen kann es zudem schnell passieren, dass Problematiken, über die Unsicherheit besteht, politisiert werden. Das heißt, es wird dann in der gesellschaftlichen Diskussion zu einer **politischen Frage, welchen Informationen geglaubt wird oder nicht**. Nicht immer stehen dann Fakten im Vordergrund, bzw. kommt es dann auf die eigene politische Haltung an, wie diese Fakten interpretiert werden.

In solchen Fällen bedeutet es eine große Verantwortung für BOS, zu entscheiden, ob man bestimmte Aussagen als Falschinformation bezeichnet oder nicht (siehe Kapitel 9.3). Denn pauschale Antworten auf diese Fragen gibt es nicht. Die Mitarbeitenden müssen hier besonders gut prüfen, auf welche Quellen sie zurückgreifen. Sie müssen sich ebenso hinterfragen, wie ihre eigenen politischen Haltungen oder andere Vorprägungen (die politische Kultur der Institution, mögliche Vorurteile) sie in ihrem Urteil beeinflussen. Gerade für Institutionen, die sachlich und politisch neutral bleiben sowie richtige Informationen teilen wollen und müssen, bedarf es hierzu Mitarbeitender, die gut ausgebildet wurden, Unterstützung bekommen und auch die Möglichkeit erhalten, mit anderen über solche schwierigen Fragen zu reflektieren.

In bestimmten Fällen kann es auch notwendig sein, **transparent zu machen, dass man als Behörde selbst gerade keine sicheren Informationen hat**. Diese Problematik erläutern wir ausgiebig in Kapitel 9.

3. Wie können BOS Falschinformationen von Meinungsäußerungen abgrenzen?



Eines der vorwiegenden Probleme bei der Bekämpfung von Falschinformationen ist es, die **Meinungsfreiheit** angemessen zu beachten. So können einzelne Äußerungen zwar inhaltlich falsch sein. Dies bedeutet aber nicht automatisch, dass sie nicht mehr der Meinungsfreiheit unterfallen. Bei möglichen Maßnahmen gegen solche Inhalte kann es also immer noch erforderlich sein, mit der Meinungsfreiheit abzuwägen, um sicherzugehen, dass die gewählte Maßnahme **verhältnismäßig** ist und die **Grundrechte der Nutzenden** hinreichend beachtet werden. Dies betrifft nicht nur die **Wahl der Maßnahme** – sei es Debunking oder auch Löschen / Blockieren von Nutzenden oder Kommentaren – sondern auch die **Art der Ausführung**. Gerade beim Löschen und Blockieren müssen Behörden vorab zwingend beachten, dass behördliche Social Media Arbeit auf ihren behördeneigenen Account beschränkt ist. **Das Vorrecht darüber hinausgehender Regulierung liegt bei den Plattformbetreibern**, wenngleich diese entsprechende Stellen zur Meldung rechtswidriger Inhalte vorbehalten müssen. Die Diskussion der Meinungsfreiheit in dem Kontext der Beschränkung von Kommentaren oder Nutzenden (siehe Kapitel 11) bezieht sich deshalb allein auf die Möglichkeit der **Moderation der eigenen Onlinepräsenz** auf diversen Plattformen.

3.1 Was umfasst die Meinungsfreiheit und wie beachte ich sie ausreichend bei Maßnahmen gegen Falschinformationen?

Jede:r soll sagen können, was sie oder er denkt, auch wenn er/sie keine nachprüfbaren Gründe für das Urteil angibt oder angeben kann. Das Grundgesetz schützt nicht nur die Meinungsfreiheit im Interesse der Persönlichkeitsentfaltung des Einzelnen (Art. 5 Abs. 1 Satz 1). Auch im Interesse des demokratischen Prozesses hat die Meinungsfreiheit eine essenzielle Bedeutung und Social Media Kanäle hoheitlicher Stellen bieten einen neue, bedeutende Plattform für den entsprechenden demokratischen Austausch. Von der Meinungsfreiheit gedeckt sind etwa Polemiken, die sich **nicht auf konkrete Personen beziehen** (wie beispielsweise ein Beitrag zu einem Sendebeitrag des MDR: “Niedrige Renten aber die Diäten für die Politik-Darsteller werden automatisch erhöht!! Da sieht man genau wo das Land steht.“; VG Leipzig, Urt. v. 11.09.2019 - 1 K 1642/18; Eggers 2020: 100 f.). **Werturteile sind grundsätzlich geschützt**, ohne dass es auf den Wert, die Emotionalität oder die Richtigkeit des Inhalts oder seine überspitzte Darstellung ankäme. Werturteile sind Äußerungen, die durch Elemente subjektiver Überzeugung oder Meinung geprägt sind und deshalb nicht wahr oder unwahr, sondern nur je nach persönlicher Überzeugung falsch oder richtig sein können. Sie sind – im Gegensatz zu Tatsachenbehauptungen, worum es sich bei Falschinformationen typischerweise hauptsächlich handelt – einem Beweis nicht zugänglich (Mafi-Gudarzi 2019: 67). Egal, ob ein Werturteil anstößig, provokativ oder unangenehm ist oder nicht, es ist automatisch von der Meinungsfreiheit geschützt. Selten bestehen Inhalte im Netz, wie Falschinformationen, jedoch alleine aus einem Werturteil. Zumeist handelt es sich um gemischte Äußerungen, also solche, die sowohl Werturteile als auch Tatsachenbehauptungen beinhalten (dazu siehe die Ausführungen unten).

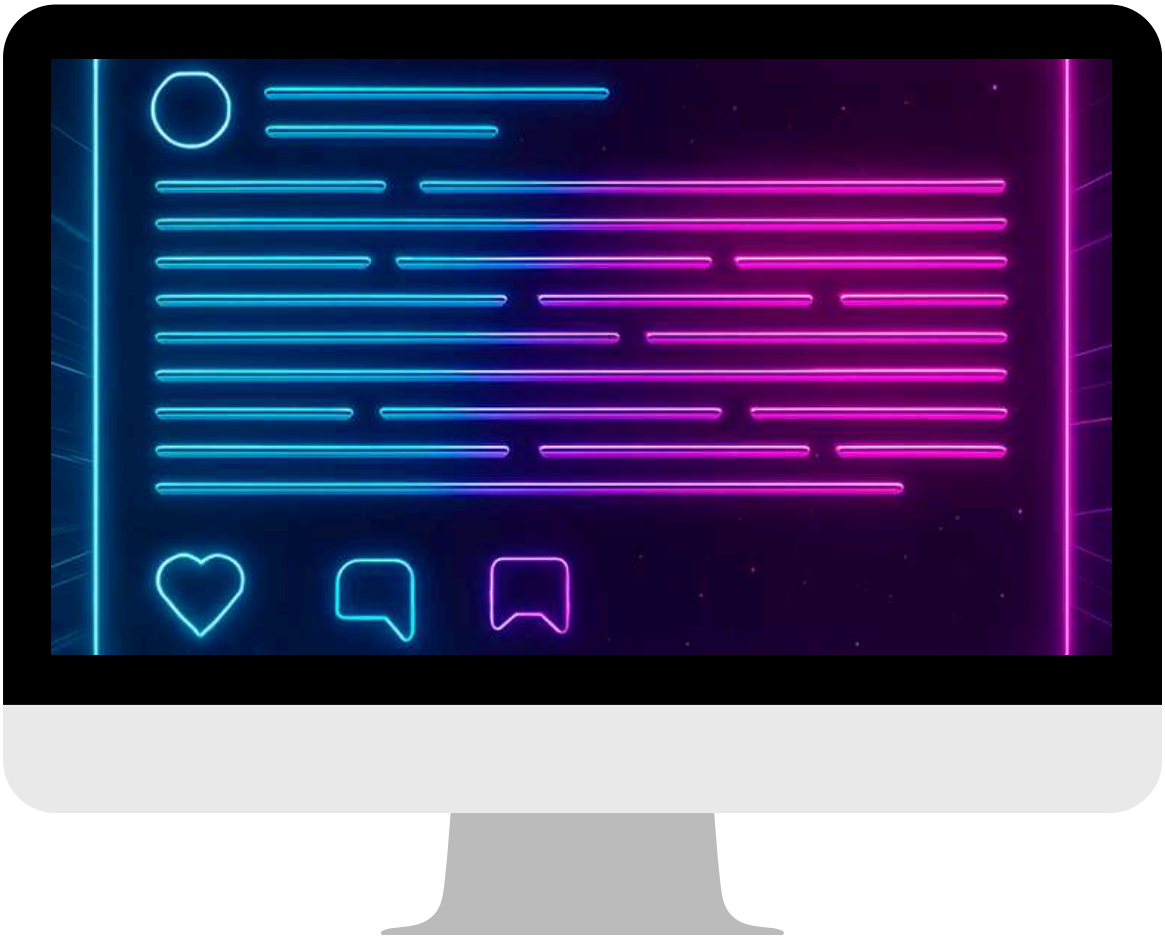
In jedem Einzelfall müssen BOS **zwischen den sich gegenüberstehenden Rechtsgütern abwägen**, bspw. der Meinungsfreiheit und der persönlichen Ehre bei Falschinformationen, die einzelne Personen anvisieren und diese diffamieren können (siehe hierzu die anschließende graphische Übersicht). Dabei müssen BOS auch den Zusammenhang, in dem die Äußerung fällt, berücksichtigen (Schwarz 2017: 244). Auch, wenn in solchen Fällen der strafrechtliche Tatbestand der Beleidigungsdelikte gem. §§ 185 ff. StGB erfüllt ist, muss eine solche Abwägung im Einzelfall vorgenommen werden. Ein solcher Ausdruck der Missachtung bzw. Nichtachtung eines anderen Menschen kann nämlich immer noch zur Ausübung der Meinungsfreiheit gem. § 193 StGB als "berechtigtes Interesse" gerechtfertigt sein. Dies kann auch ein **Beitrag zum geistigen Meinungskampf in einer die Öffentlichkeit wesentlich berührenden Frage** sein. Je bedeutender dann die Diskussion für die Öffentlichkeit ist, desto eher kann die Meinungsfreiheit ehrverletzende Äußerungen rechtfertigen.

Auch die Möglichkeit einer **Kritik an der Ausübung staatlicher Gewalt** kann die personalisierte herabsetzende Äußerung gegen Amtsträger rechtfertigen (Eggers 2020: 102 f.). Sollten im Rahmen einer Demo etwa Nutzende das Vorgehen der Polizei kritisieren wollen und dafür auch einzelne Polizist:innen hervorheben und abwertend über diese speziell reden, kann dies immer noch rechtmäßig sein. Zusätzlich zu berücksichtigen sind bei privaten Diskutierenden die **Diskussionskultur des genutzten Netzwerks und die gewählte Öffentlichkeit** des Forums. In bestimmten Foren kann es etwa üblich sein, eine verrohte Sprache zu benutzen, weshalb der ehrverletzende Charakter einer Äußerung entsprechend bewertet werden muss. Zugleich wird die Verletzung der persönlichen Ehre durch die besondere Öffentlichkeit eines Posts außerhalb eines bilateralen Chats intensiver verletzt.

Wegen letzterem ist dann nämlich regelmäßig nicht die enge Privatsphäre, sondern die **Sozialsphäre** betroffen und gewisse schärfere Reaktionen müssen hingenommen werden. Unter der Sozialsphäre versteht man im allgemeinen Persönlichkeitsrecht neben der Öffentlichkeitssphäre, der Privatsphäre und der Intimsphäre eine der vier Sphären der Persönlichkeit. Die Sozialsphäre ist jene Sphäre, in der Menschen mit anderen sozial interagieren. Unter Privatsphäre versteht man den Bereich eines Menschen, in dem er unter Ausschluss der Öffentlichkeit das Recht auf freie Entfaltung seiner Persönlichkeit hat. Der Rechtfertigungsaufwand wäre bei Maßnahmen, die in diesen Bereich eingreifen, entsprechend höher als bei der Sozial- oder Öffentlichkeitssphäre (GG-Paulus, Art. 5 Rn. 329 ff.). BOS müssen immer **im Einzelfall klären**, ob Werturteile oder Tatsachenbehauptungen so ehrverletzend sind, dass sie sich abträglich auf das Ansehen und Bild der/des Betroffenen in der Öffentlichkeit auswirken.

.

Nach dem virtuellen Hausrecht dürfen Plattformen, aber auch BOS (allerdings nur auf ihren eigenen Accounts) sog. **Schmähkritiken bzw. Formalbeleidigungen** entfernen, bei denen die Herabsetzung besonders schwer wiegt und die Diffamierung einer Person gerade im Vordergrund steht, sowie **unwahre Tatsachenbehauptungen**, deren Unwahrheit die/der Äußernde zum Zeitpunkt der Äußerung kennt oder deren Unwahrheit erwiesen ist. Bei solchen Äußerungen besteht in der Regel kein schützenswertes Interesse im Sinne der Meinungsfreiheit; sie fällt nicht in die "Waagschale" der Abwägung (Fechner 2023: 53, 67). Eine Abwägung zwischen der Meinungsfreiheit und den Persönlichkeitsrechten findet bei erwiesen oder bewusst unwahren Tatsachenbehauptungen also zwar nicht statt, es muss jedoch vorher klar geprüft werden, ob es sich um den Fall einer solchen Äußerung handelt. Ein Merkmal hierfür kann fehlender konkreter Sachbezug zur Diskussion sein.



.

Bei **gemischten Äußerungen**, die sowohl wertende als auch tatsächliche Elemente beinhalten und damit grundsätzlich in den Schutzbereich der Meinungsfreiheit fallen können, fällt der **Wahrheitsgehalt der Äußerungen** ins Gewicht (BeckOK InfoMedienR-Söder, § 823 BGB Rn. 45 f.). Häufig handelt es sich bei Falschinformationen um genau solche. Sind Teile der Äußerung erwiesen falsch oder sogar bewusst unwahr, tritt regelmäßig die Meinungsfreiheit zurück und eine Löschung der Behauptung oder die Blockade der/des Nutzers/in ist legitim. Dabei ist es aber ebenfalls wichtig, dass BOS wiederum zwischen den Alternativen der Löschung und der Blockade unterscheiden und beachten, dass zwischen diesen beiden Maßnahmen ein Stufenverhältnis besteht. Das Löschen einzelner Behauptungen wiegt in der Regel weniger schwer als die Blockade der/des Nutzenden. Im Einzelfall müssen BOS also wiederum abwägen, ob bspw. die Blockade noch verhältnismäßig ist, oder sie sich effektiv und rechtmäßig mit der Löschung behelfen können. Wollen BOS diese Maßnahmen vornehmen, beschränkt sich dies aber weiterhin auf die eigene Onlinepräsenz (mehr hierzu im Kapitel 11). BOS haben nicht nur ein Recht zur Moderation eigener Accounts, es ist auch eine verfassungsrechtliche Pflicht staatlich geführter Accounts, rechtswidrigen Inhalten angemessen zu begegnen. Diese Pflicht leitet sich bereits aus der Schutzpflichtdimension potenziell betroffener Grundrechte her. Grundrechte stellen nicht nur subjektive Abwehrrechte gegen den Staat dar, sondern verpflichtet ihn darüber hinaus auch objektiv, die potenzielle Freiheitsentfaltung seiner Bürger:innen so zu fördern, dass die Freiheiten auch real wahrgenommen werden können (Dreier/Kaiser, GG, Art. 5 Abs. 1 Rn. 192). Die Öffentlichkeitsarbeit ist notwendig, “um den Grundkonsens im demokratischen Gemeinwesen lebendig zu erhalten und die Bürger:innen zur eigenverantwortlichen Mitwirkung an der politischen Willensbildung sowie der Bewältigung vorhandener Probleme zu befähigen” (BVerfG, Urt. v. 27. Februar 2018 - 2 BvE 1/16).

Zugunsten der Persönlichkeitsentwicklung und Ausübung der Meinungsfreiheit von Nutzenden oder der Förderung der Informationsfreiheit kann deshalb im Einzelfall die Pflicht staatlicher Behörden erwachsen, rechtswidrige Inhalte in verhältnismäßiger Weise zu regulieren. Überwiegen im Einzelfall Schutzinteressen von Betroffenen an der Wahrung ihrer (Grund-)Rechte oder das Ziel der Wahrung der öffentlichen Sicherheit, besteht somit sogar eine aus der staatlichen Schutzpflicht erwachsende Verpflichtung zur Löschung des entsprechenden Inhalts.

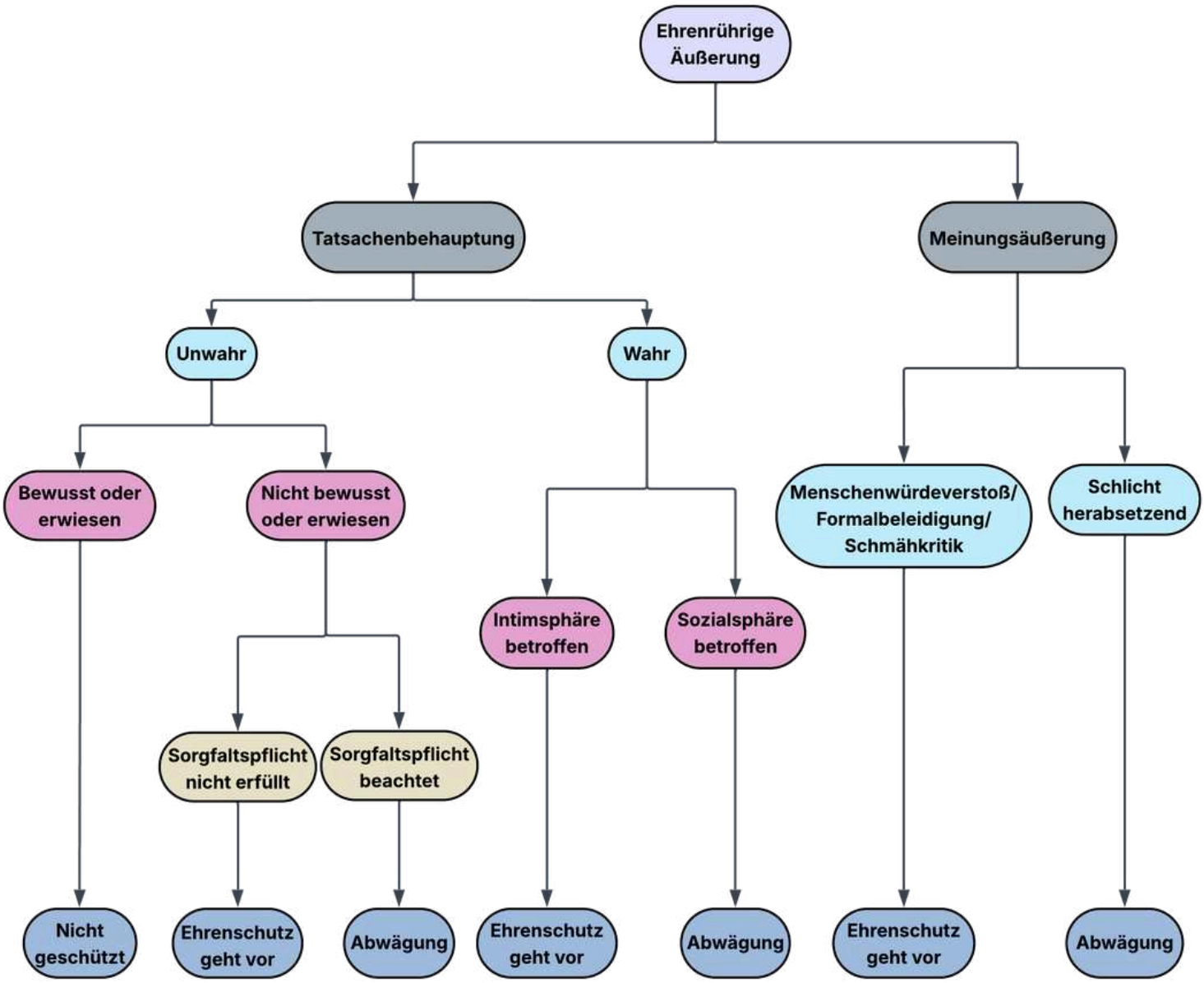


Abbildung 1: Beispielhafte Darstellung der Abwägung mit der Meinungsfreiheit anhand ehrverletzender Äußerungen

Quelle: Eigene Abbildung, nach *Grimm*, "Die Meinungsfreiheit in der Rechtsprechung des Bundesverfassungsgerichts", NJW 1995, 1697, 1705

3.2 Der Sonderfall “Shitstorm” gegen die eigene Einrichtung

Ein schwieriges Feld sind auch die **Angriffe auf behördlichen Accounts** oder Foren, bei denen sich Nutzende über die jeweilige Einrichtung beschweren. Kompliziert ist dann die Abgrenzung zu duldender, möglicherweise polemischer Äußerungen von nicht zu duldenden Inhalten, bei denen das virtuelle Hausrecht geltend gemacht werden kann. Bei Ersteren ist es weder erlaubt, Maßnahmen gegen die Inhalte zu ergreifen noch selbst zu polemischen Gegenangriffen auszuholen. Natürlich ist aber eine sachliche Antwort nicht nur erlaubt, sondern aus dem Gedanken der Transparenz der Öffentlichkeitsarbeit auch geboten. Nicht dulden müssen BOS hingegen solche Äußerungen, die **die Funktion der Einrichtung beeinträchtigen** (Eggers 2020: 108 f.). In Fällen von Falschinformationen, welche strafrechtliche Relevanz besitzen, wie beleidigende Inhalte, kann ein Strafantrag gestellt werden. Darüber hinaus gibt es auch Fälle schwerwiegender Beeinträchtigungen, durch die das Mindestmaß an öffentlicher Anerkennung einer öffentlichen Einrichtung derart beschädigt wird, dass sie ihre Funktion nicht mehr erfüllen kann, weil das unerlässliche Vertrauen in ihre Integrität in Frage gestellt wird. Trotz fehlender „persönlicher Ehre“ einer solchen Einrichtung, weil sie nun einmal als Einrichtung nicht in den Schutzbereich der entsprechenden Grundrechte fällt, führt dies dazu, dass die Behörde ihre gemeinnützige Aufgabe nicht erfüllen kann. Neben strafverfolgungsrechtlichen Möglichkeiten könnte eine Behörde dann ebenfalls einen zivilrechtlichen Unterlassungsanspruch geltend machen (BGH, Ur. v. 16. November 1982 - VI ZR 122/80), woraus sich ebenfalls das Recht der Behörde ergibt, derart rechtswidrige Äußerungen hausrechtlich auf ihren eigenen Accounts zu löschen. Bei Presseberichten, die unwahre Tatsachenbehauptungen über Handlungen der öffentlichen Einrichtung enthalten und durch Nutzende verbreitet werden, kommt zudem ein presserechtlicher Gegendarstellungsanspruch in Betracht, welche die betroffene Behörde im Verlauf von Diskussionen ebenfalls weiterverbreiten kann (Eggers 2020: 110).

Die Lösungen zu den folgenden praktischen Übungen finden Sie auf den Seiten 168 f.

Fallbeispiel 1
Abwägung Ehre — Meinungsfreiheit
BVerfG, Beschluss v. 12. Mai 2009, Az. 1 BvR 2272/04

In diesem Fallbeispiel geht es zwar nicht explizit um eine Falschinformation. Es verdeutlicht jedoch praktische Abwägungen im Rahmen von Meinungsäußerungen.

Der Journalist und Mitherausgeber einer Zeitung – T – äußerte sich als Diskussionsteilnehmer einer Talkshow mit dem Thema „F. – die Öffentlichkeit und die Moral“ zum Ermittlungsverfahren gegen den damaligen Vizepräsidenten des Zentralrates der Juden wegen des Verdachts des unerlaubten Umgangs mit Betäubungsmitteln folgendermaßen:

„Und ich bin ganz sicher, dass dieser staatsanwaltliche, man muss wirklich sagen: Skandal eines ganz offenkundig, ich sag’s ganz offen, durchgeknallten Staatsanwaltes, der hier in Berlin einen außerordentlich schlechten Ruf hat, der vor einem Jahr vom Dienst suspendiert worden ist, der zum ersten Mal überhaupt wieder tätig wird. Dieser Skandal wird zweifellos dazu führen, dass sich die hiesige Justizbehörde und die ihr zugeordnete Staatsanwaltschaft fragen muss, ob man auf diese Art und Weise gegen Privatpersonen vorgehen kann.“

Müssen hier das Persönlichkeitsrecht des Staatsanwalts und die Meinungsfreiheit des T miteinander abgewogen werden? Um welchen Sonderfall ehrverletzender Äußerungen könnte es sich hier handeln?

Fallbeispiel 2
VG Mainz, Urteil v. 13. April 2018, Az. 4 K 762/17.MZ

Zur Diskussion um den Zuzug von Flüchtlingen äußerte sich der Nutzer T auf dem Facebook-Profil „ZDF Heute+“ gegenüber namentlich angesprochenen Nutzenden folgendermaßen:
„Mir ist jeder kriminelle Ausländer lieber als so ein linkes Drecks- Geschmeiß wie Ihr! Ihr seid Abschaum, den man lebendig einbetonieren sollte! Ihr seid beide so hässlich, da ist selbst die Bezeichnung Untermensch noch schmeichelhaft.“
„Tja leider hast Du Deine Bilder nicht gesperrt und so sieht man, dass Du eigentlich fett, alt und hässlich bist. Deine geistige Engstirnigkeit kommt ja nun nachweislich noch dazu.“
Wäre eine Sperrung des Nutzers auf dem eigenen Account legitimierbar?

Fallbeispiel 3
Angriffe gegen eine Einrichtung
BGH, Urteil v. 16. November 1982, Az. VI ZR 122/80
(„Vetternwirtschaft“)

In einem Schreiben an die damalige Bundesagentur für Arbeit behauptete der Bürger B Folgendes:
„Sie haben nachweislich unbefugt auf der Basis von Günstlings- und Vetternwirtschaft in Reinkultur öffentliche Gelder verschwendet, indem Sie mit nichts gerechtfertigte Arbeitslosengelder an Frau G. auszahlten.“
Weiter drohte der B damit, seine Behauptung öffentlich zu machen. Die Bundesagentur für Arbeit konnte die Unwahrheit der Behauptungen überzeugend nachweisen.
Welche Interessen hat die Behörde in diesem Zusammenhang und wie sind sie mit der Meinungsfreiheit des Bürgers B abzuwägen? Um welche im Text erwähnte Sonderkonstellation handelt es sich und was folgt daraus?

Die Lösungen zu diesem Quiz finden Sie auf Seite 169.

Frage 1

Welche Art von Äußerungen fallen unter das virtuelle Hausrecht und können entsprechend gelöscht werden?

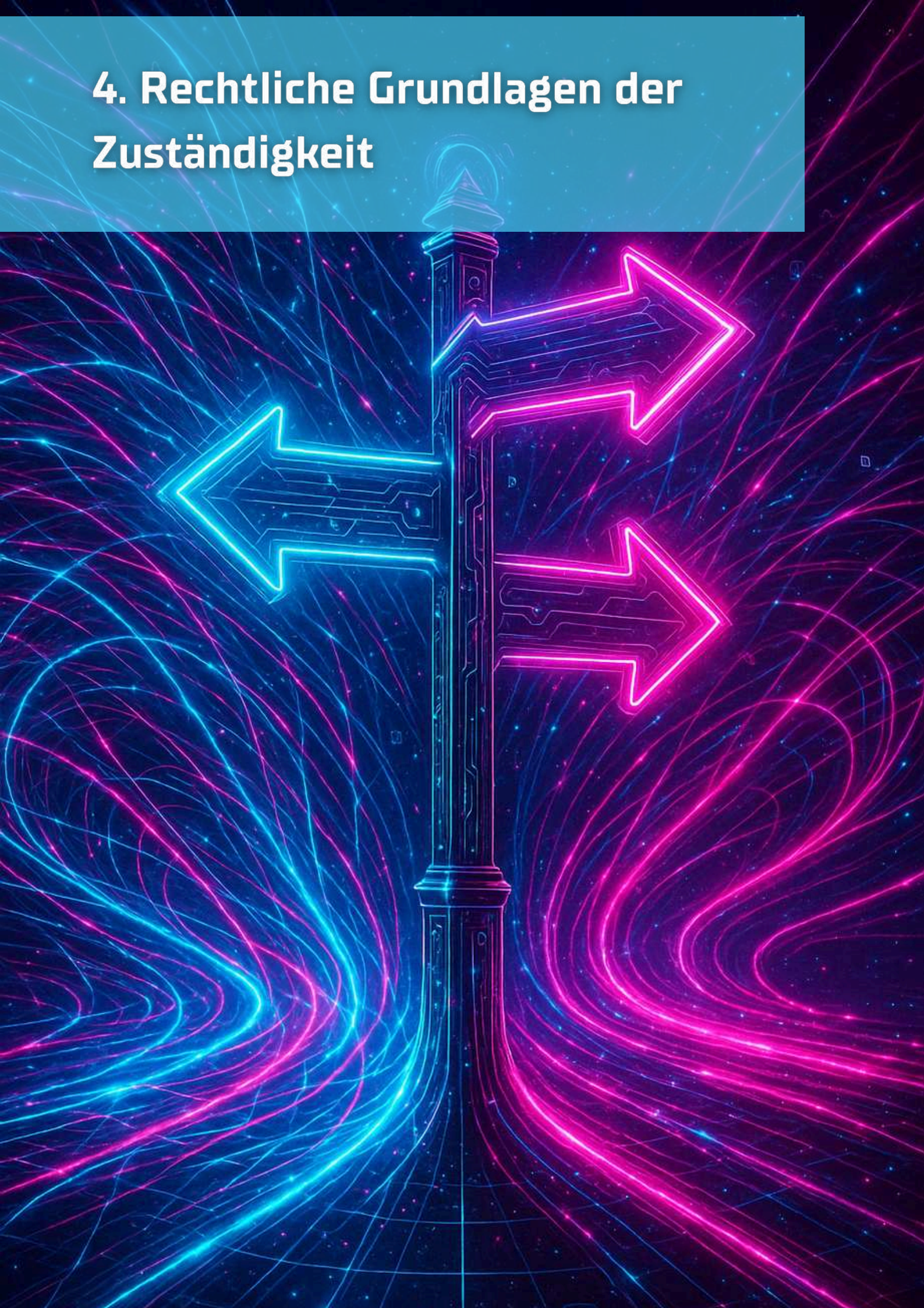
a) Äußerungen, die den Tatbestand der Beleidigungsdelikte gem. §§ 185 ff. StGB erfüllen
b) Werturteile ohne konkreten Sachbezug
c) Polemische Kommentare
d) Erwiesen oder bewusst unwahre Tatsachenbehauptungen

Frage 2

Was könnte eine Behörde unternehmen, wenn unwahre Tatsachenbehauptungen über sie verbreitet werden? (mehrere Antwortmöglichkeiten)

a) Eine strafrechtliche Anzeige gegen die Verbreitenden erstatten
b) Polemische Gegenangriffe starten
c) Einen zivilrechtlichen Unterlassungsanspruch geltend machen
d) Die Nutzenden auf der Plattform blockieren

4. Rechtliche Grundlagen der Zuständigkeit



4.1 Hintergrund

Falschinformationen treten in unterschiedlichsten Kontexten und über eine Vielzahl von Kanälen auf. Die gezielte Verbreitung falscher oder irreführender Informationen (sog. Desinformation) kann dabei sowohl auf nationaler als auch auf internationaler Ebene erfolgen. Sie dient häufig dem Ziel, öffentliche Meinungen zu beeinflussen, Konflikte zu schüren oder institutionelles Vertrauen zu untergraben. Aufgrund dieser unterschiedlichen Kontexte variieren auch die Zielsetzungen von Maßnahmen zur Bekämpfung von Desinformation. Sie hängen maßgeblich davon ab, ob Desinformationen individuelle Rechtsgüter, die geschriebene Rechtsordnung oder aber den Staat als solchen betreffen. Darüber hinaus ist Misinformation gerade in Gefahrenlagen weit verbreitet, also nicht intendierte Falschinformationen wie beispielsweise Gerüchte und Spekulationen (siehe Kapitel 1.1).

Die unterschiedlichen Kontexte dieser verschiedenen Arten der Falschinformationen erfordern entsprechend verschiedene Akteure und Gegenmaßnahmen. Betreiber von Internetplattformen können beispielsweise verpflichtet werden, strafrechtlich relevante Inhalte zu löschen oder irreführende Inhalte zu kennzeichnen. Strafverfolgungsbehörden müssen beispielsweise tätig werden, soweit strafbare Handlungen aufzuklären sind, während sich überregionale Behörden auf die Bekämpfung von Desinformationskampagnen fokussieren.

Im deutschen Verwaltungsrecht wird dabei zwischen drei grundlegenden Zuständigkeitsarten unterschieden: der sachlichen, der örtlichen und der instanziellen Zuständigkeit. Während die sachliche Zuständigkeit vor allem die Frage betrifft, welche Behörde für eine bestimmte Aufgabe zuständig ist, legt die örtliche Zuständigkeit den räumlichen Bereich fest, innerhalb dessen eine Behörde tätig werden darf. Die instanzielle Zuständigkeit befasst sich sodann mit den verschiedenen Ebenen innerhalb eines Verwaltungszweiges.

Für die Bekämpfung von Desinformation ist vor allem die **sachliche Zuständigkeit** von Interesse. Bedroht Desinformation die öffentliche Sicherheit und Ordnung, finden sich Rechtsgrundlagen zum Handeln im allgemeinen Gefahrenabwehrrecht. Die öffentliche Sicherheit umfasst dabei den Schutz der Rechtsordnung, den Schutz individueller Rechtsgüter wie Leben, Gesundheit, Freiheit oder Eigentum und den Schutz des Staates und seiner Einrichtungen. Falschinformationen können für sämtliche dieser Bereiche eine Gefahr darstellen. Werden im Internet etwa Falschinformationen über medizinische Themen verbreitet, etwa zu Impfstoffen und Medikamenten, kann dies zu gesundheitlichen Risiken und damit Gefahren für individuelle Rechtsgüter führen. Gezielte Desinformationen über Einzelpersonen können dagegen verleumderisch und rufschädigend wirken und individuelle Persönlichkeitsrechte verletzen. Desinformation kann aber ebenso zu Gewalt oder Straftaten anstacheln, wodurch die öffentliche Sicherheit beeinträchtigt wird (siehe vertiefend Kapitel 1.7).

4.2 Zuständigkeiten einzelner BOS

4.2.1 Polizei und Ordnungsbehörden

Für die Bereiche der öffentlichen Sicherheit und Ordnung sind grundsätzlich sowohl die Ordnungsämter als auch die Polizei zuständig. Entsprechende Regelungen finden sich in den jeweiligen Polizei- und Ordnungsbehördengesetzen der Länder (etwa § 1 OBG NRW, § 1 Abs. 1 PolG NRW). Diese ermächtigen Polizei und Ordnungsbehörden unter anderem dazu, Maßnahmen zur Gefahrenabwehr zu treffen. Dabei bestehen für beide Behörden Generalklauseln als Ermächtigungsnormen für Fälle, die nicht durch spezielle Rechtsvorschriften geregelt sind. Weil Ordnungsbehörden und Polizei somit jeweils entsprechende Befugnisse zur Gefahrenabwehr haben, besteht ein zu lösendes Konkurrenzverhältnis.

Die Polizei ist zudem gemeinsam mit den Staatsanwaltschaften für die Verfolgung von **Straftaten** im Zusammenhang mit Desinformationen zuständig. Inwieweit die Verbreitung von Falschinformationen strafrechtlich verfolgt werden kann, ist allerdings eine Frage des Einzelfalles. Nicht jede solche Verbreitung ist per se strafbar. Geht es etwa um strategische Desinformationskampagnen als Angriff auf die demokratische Willensbildung, greifen Straftatbestände wie die üble Nachrede (§ 186 StGB), Verleumdung (§ 187 StGB) oder Volksverhetzung (§ 130 StGB) regelmäßig nicht, weil es keine konkreten Adressat:innen gibt und weitere erforderliche Tatbestandsmerkmale, wie etwa ein Gruppenbezug, nicht gegeben sind (Schlömer und Kehrberg 2025, 5). Anders sieht dies bspw. aus, wenn ein anonymer Account in einer Chatgruppe gezielt die Falschinformation verbreitet, dass eine bestimmte religiöse Minderheit für die mutmaßliche Verbreitung eines Virus verantwortlich sei und man diese Gruppe deshalb “aus dem öffentlichen Leben entfernen” müsse. Hier liegt eine gruppengerichtete Äußerung vor, die nicht nur eine Falschbehauptung, sondern zugleich einen Aufruf zur Ausgrenzung und zu Hass gegen eine Bevölkerungsgruppe darstellt. Damit könnte der Straftatbestand der Volksverhetzung (§ 130 StGB) erfüllt sein, wenn die Aussage zugleich geeignet ist, den öffentlichen Frieden zu stören. Im Falle fehlender strafrechtlicher Relevanz können Falschinformationen allerdings weiterhin die öffentliche Sicherheit und Ordnung gefährden. Eine Zuständigkeit der Polizei kann sich damit dennoch auf Grundlage der Gefahrenabwehr ergeben.

Die Ordnungsbehörden fungieren im Verhältnis zur Zuständigkeit von Polizeibehörden als “reguläre“ Gefahrenabwehrbehörden. Die Polizei ist in diesen Bereichen sachlich zuständig, wenn eine Gefahr dringend ist und die Ordnungsbehörde nicht rechtzeitig handeln kann (**Eilfallkompetenz**), oder wenn polizeiliche Mittel und Befugnisse erforderlich sind. Polizei und Ordnungsbehörden müssen demnach eine Verlaufsprognose darüber anstellen, ob die Gefahrenabwehr durch die Ordnungsbehörden bewältigt werden kann. Auch die (präventive) Verhinderung der Verbreitung von Falschinformationen durch ein Erteilen von Auflagen gegen Veranstalter:innen bei kommunalen Events kann durch Ordnungsbehörden erfolgen. Es geht demnach um die Bewältigung kommunaler Aufgaben, bei denen keine akute Gefahr besteht. Wird allerdings ein bewaffneter Angreifer im Stadtzentrum gesichtet oder wird zu Straftaten oder Gewalt aufgerufen, ist die Polizei sachlich zuständig, weil hier dringende Gefahren für Leib oder Leben bestehen, die kein weiteres Abwarten zulassen. Der Zuständigkeitsbereich der Ordnungsbehörden ist im Bereich von Falschinformationen somit letztlich begrenzt. Ordnungsbehörden sind nur (mit) zuständig, wenn Falschinformationen Auswirkungen auf die öffentliche Sicherheit und Ordnung unmittelbar vor Ort haben. Allerdings besitzen Ordnungsbehörden nicht die rechtlichen und technischen Mittel, um systematisch gegen Falschinformationen im Internet oder auf überregionaler Ebene vorzugehen. Sie sind daher nicht primär für die Bekämpfung von Falschinformationen zuständig, sondern arbeiten meist unterstützend.

Je nach Organisation der einzelnen Gemeinden kann es auch dazu kommen, dass das Ordnungsamt nur während der gewöhnlichen Arbeitszeiten aktiv ist, beispielsweise nur montags bis freitags tagsüber. In derartigen Fällen übernimmt die Polizei die Aufgaben der Ordnungsbehörden, etwa bei nächtlicher akuter Gefahrenabwehr durch Ruhestörungen. Hierneben kann es auch dazu kommen, dass die Ordnungsbehörden die Polizeibehörden um **Vollzugshilfe** bitten.

Im Rahmen der sachlichen Zuständigkeit gilt das **allgemeine Subsidiaritätsprinzip**. Ordnungsbehörden dürfen Maßnahmen zum Schutz privater Rechte nur ergreifen, wenn es keine Möglichkeit gibt, rechtzeitig gerichtliche Hilfe zu bekommen. Das heißt, sie dürfen nur dann eingreifen, wenn ohne ihre Unterstützung ein entsprechendes Recht von Personen gar nicht durchgesetzt werden kann oder es erheblich schwieriger wäre. Falschbehauptungen auf Social Media über eine Person, die ihren Ruf schädigen können, fordern somit nach dem allgemeinen Subsidiaritätsprinzip, dass Personen zunächst selbst die entsprechenden Plattformen kontaktieren und Inhalte melden. Möglicherweise können auch diejenigen Personen, welche die Desinformation verbreitet haben, zum Löschen aufgefordert werden.

Eine **Ausnahme** vom Subsidiaritätsprinzip ist jedoch unter anderem anerkannt, wenn die Individualrechtsgüter einer unbestimmten Vielzahl von Personen bedroht werden. Denn bei einer Bedrohung von vielen Personen bzw. vielen Rechten besteht ein erhebliches öffentliches Interesse an der Gefahrenabwehr. Je nach Inhalt, Plattform und Viralität der Falschinformation ist letzterer Fall aufgrund der besonderen Öffentlichkeit im Netz durchaus naheliegend. Falschinformationen können bei größeren Gruppen von Menschen Panik auslösen, was ein rasches und zentrales Eingreifen erfordert, weil die Selbstverantwortung Einzelner nicht mehr zur Gefahrenbewältigung ausreicht.

Das Verhältnis der Zuständigkeiten zwischen der **Bundespolizei** und den Landespolizeibehörden lässt sich wie folgt beschreiben: Generell gilt eine allgemeine Polizeihoheit der Länder. Diese wird lediglich in den Bereichen verdrängt, die in den sachlichen Zuständigkeitsbereich der Bundespolizei fallen (Bäcker 2021 Rn. 167 ff.). Dieser umfasst insbesondere die Gewährleistung der Sicherheit im Bahn- und Luftverkehr und den Grenzschutz, aber auch weitere Aufgaben, wie Sicherheitsmaßnahmen auf See außerhalb des deutschen Küstenmeeres entsprechend der Befugnisse des Völkerrechtes sowie Auslandseinsätze, sei es im Rahmen internationaler polizeilicher Kooperationen oder durch eigenständige Maßnahmen in spezifischen Fällen. Aufgrund dieser eindeutigen Abgrenzung der sachlichen Zuständigkeiten bestehen keine Weisungsbefugnisse der Bundespolizei gegenüber den Landespolizeibehörden. Die Bundespolizei wäre demnach aber für Falschinformationen zuständig, die in ihren besonderen Aufgabenbereich fallen. Denkbar wäre etwa, dass über soziale Medien gezielte Falschinformationen darüber verbreitet werden, dass ein Terroranschlag auf einen deutschen Flughafen bevorsteht. Das kann eine Panik auslösen, die die Sicherheit an dem betreffenden Ort massiv beeinträchtigt. In einem derartigen Fall überprüft und bewertet die Bundespolizei die Bedrohungslage und kann etwa Reisende und deren Gepäck kontrollieren. Auch kann sie im Rahmen ihrer Zuständigkeit für die Gewährleistung der Sicherheit des Luftverkehrs über offizielle Kanäle im Internet kommunizieren und Richtigstellungen verbreiten.

4.2.2 Bundeskriminalamt (und Landeskriminalämter)

Das Bundeskriminalamt (BKA) stellte nach ursprünglicher Idee zunächst eine Zentralstelle als Bindeglied zwischen den Landeskriminalämtern dar. Die einzelnen Aufgaben der Landeskriminalämter ergeben sich aus den jeweiligen Gesetzen der Länder. Regelmäßig leiten und steuern sie komplexe Ermittlungen und beraten und unterstützen die örtliche Polizei. Häufig ermitteln die Landeskriminalämter in Fällen schwerer Kriminalität, etwa in Fällen schwerer Straftaten, wie Mordserien und Sexualdelikten, auch selbst.

Vor dem Hintergrund zunehmender europäischer und internationaler Kooperationen erweitern sich allerdings auch die Aufgaben des BKA (Barczak 2023a Rn. 13). Im Kontext der Bekämpfung von internationalem **Terrorismus** nimmt das BKA als „Sonderpolizei des Bundes“ (BVerfGE 97, 198, 218; Barczak 2023a Rn. 10) eine eigenständige Zuständigkeit wahr. Im digitalen Raum ist das BKA insbesondere auch für den Erlass und die Überprüfung von Entfernungsanordnungen zur Bekämpfung der Verbreitung terroristischer Online-Inhalte zuständig (Barczak 2023b Rn. 60).

Im Bereich der Strafverfolgung nimmt das BKA nach § 4 BKAG bestimmte polizeiliche Aufgaben wahr, etwa bei **politischen Attentaten** zum Nachteil von Verfassungsorganen oder bestimmten **international organisierten Straftaten**. Als Schnittstelle wird das BKA darüber hinaus vor allem relevant für desinformationsbezogene Straftaten, **staatlich gelenkte Propaganda oder grenzüberschreitende Desinformationskampagnen**. Es kann etwa die Ermittlungen übernehmen, insbesondere wenn sich Täter:innen im Ausland aufhalten und Straftatbestände wie die Volksverhetzung (§ 130 StGB) oder die öffentliche Aufforderung zu Straftaten (§ 111 StGB) im Raum stehen. Das BKA unterstützt die Landeskriminalämter bei der Aufklärung spezifischer Straftaten und agiert insbesondere bei der Prävention und Bekämpfung von **Cyberkriminalität**, beispielsweise durch die Identifikation und Neutralisierung automatisierter Programme zur Verbreitung von Desinformation sowie bei der Abwehr von Hacking-Angriffen und Cyberattacken.

4.2.3 Bundesamt für Verfassungsschutz

Das Bundesamt für Verfassungsschutz (BfV) ist sachlich zuständig für die Überwachung von Desinformation **außerhalb der Gefahrenabwehr im Einzelfall**. Es versteht sich selbst als „Frühwarnsystem“, indem es Methodik, Mechanismen und Wirkung von entsprechenden Operationen identifiziert und gegenüber Parlament, Regierung und Öffentlichkeit Bericht erstattet (BfV 2023). Zu beachten ist hierbei das **Trennungsgebot** zwischen Polizei und BfV. Die Befugnisse von diesen Institutionen dürfen nicht deckungsgleich sein, um eine mögliche Wiederauferstehung der Gestapo zu vermeiden. Nachrichtendienste dürfen keine Befugnisse der Polizei wahrnehmen. Aufgabe des Verfassungsschutzes ist nicht die Gefahrenabwehr, sondern die Vorbereitung der rechtzeitigen Abwehr durch die zuständigen Behörden, u. a. eben die Polizeibehörden. Insofern ist auch organisatorisch jegliche Angliederung oder Verbindung zwischen Polizei und Verfassungsschutz verboten. Weder in die eine noch in die andere Richtung besteht eine Weisungsbefugnis zwischen den Behörden.

Dennoch gibt es **zwei Ausnahmen** von dieser Trennung: Zum einen überschneiden sich die Aufgabenbereiche von Polizei und Verfassungsschutz. Soweit die Polizeibehörden auch **sach- und personenbezogenen Daten erheben und verarbeiten,** um ihre Abwehrtätigkeit auszuführen, und dabei auf einen zwischenbehördlichen Austausch von Informationen angewiesen sind, können sich ihre Befugnisse mit der Beobachtungs- und Aufklärungsarbeit des Verfassungsschutzes überschneiden. Der entscheidende Unterschied zwischen den Befugnissen zeigt sich darin, dass die Polizei ihre Maßnahmen gegen Individuen richten und im Zweifel auch mit Zwang durchsetzen kann.

Der Verfassungsschutz dagegen ist eine reine Nachrichtendienstbehörde ohne polizeiliche Befugnisse und darf vor diesem Hintergrund keine Maßnahmen mit Zwang, wie Durchsuchungen, Festnahmen oder Beschlagnahmungen durchführen. Zum anderen gibt es auch Überschneidungen zwischen der Arbeit des Verfassungsschutzes und der Polizeibehörden im Rahmen **der informationellen Zusammenarbeit, wenn diese gesetzlich klar begrenzt ist**, wie im Fall des **Antiterrordateigesetzes** (ATDG). Ziel dieser Zusammenarbeit ist die Bündelung relevanter Informationen zur gemeinsamen Abwehr des internationalen Terrorismus. Insofern ist die Desinformation wieder im Einzelfall nach Inhalt, Plattform sowie Viralität und dem daraus hervorgehenden Gefährdungspotenzial zu bewerten, um festzustellen, ob der Verfassungsschutz, eine Polizeibehörde, oder beide zuständig sind.

4.2.4 Bundesnachrichtendienst

Neben dem Bundesamt für Verfassungsschutz kann auch der Bundesnachrichtendienst (BND) gegen Desinformation aktiv werden, allerdings nur in klar abgegrenzten Zuständigkeitsbereichen. Als Auslandsnachrichtendienst Deutschlands agiert der BND im Rahmen seiner gesetzlichen Aufgaben **ausschließlich im Ausland oder bei grenzüberschreitenden Sachverhalten**. Zur Tätigkeit im Inland ist der BND nicht befugt. Allerdings kann es zu einem grenzüberschreitenden Sachverhalt kommen, wenn Desinformationskampagnen aus dem Ausland gesteuert werden und die öffentliche Meinung in Deutschland beeinflussen soll. In derartigen Fällen ist der BND für die Beschaffung und Auswertung von Informationen aus dem Ausland zuständig.

4.2.5 Bundesamt für Sicherheit in der Informationstechnik

Als Cybersicherheitsbehörde des Bundes dient das Bundesamt für Sicherheit in der Informationstechnik (BSI). Die Behörde im Geschäftsbereich des Bundesinnenministeriums ist unter anderem zuständig für die Gestaltung einer sicheren Digitalisierung in Deutschland. Ihr Aufgabenkatalog in § 3 BSIG umfasst verschiedene Elemente zur Abwehr von Gefahren für die Informationstechnik des Bundes. Im Bereich Desinformation fällt in ihren Aufgabenbereich etwa die **technische Analyse von Cyberangriffen**, die mit Desinformationen gekoppelt sein können. Gleichzeitig liefert das BSI **Informations- und Beratungsangebote**, wie beispielhaft im Rahmen anstehender Wahlen zum Schutz vor illegitimer Beeinflussung (BSI 2025).

4.2.6 Bundesnetzagentur

Der **Digital Services Coordinator (DSC)** bei der Bundesnetzagentur ist die zentrale Koordinierungsstelle für die Durchsetzung des Digital Services Act (DSA) in Deutschland. Der DSA selbst verpflichtet digitale Dienste und Online-Plattformen zu Sorgfalt und Transparenz im Netz durch das Ergreifen von Maßnahmen gegen rechtswidrige Inhalte. Dadurch ermöglicht er es, einfacher gegen illegale Inhalte, Hass und Hetze und gegen Desinformation vorzugehen, soweit es sich hierbei um vom DSA erfasste *rechtswidrige* Inhalte handelt. Der DSA verfolgt dabei den Ansatz, dass die Rechtsdurchsetzung zunächst auf privatem Weg zu verfolgen ist und den digitalen Diensten und Online-Plattformen hierbei eine Eigenverantwortung obliegt (Kuhlmann und Trute 2022, 116). Demnach müssen Privatpersonen rechtswidrige Inhalte zunächst an die Plattformen melden, die diese dann entfernen müssen. Große Online-Plattformen müssen darüber hinaus auch Risikobewertungen durchführen und eigenständig risikominimierende Maßnahmen ergreifen (Schlömer und Kehrberg 2025, 4). Tun sie dies nicht, können letztere zur Durchsetzung des DSA allerdings auch mit Sanktionen belegt werden. Gleichzeitig sieht Art. 9 DSA vor, dass nationale Justiz- oder Verwaltungsbehörden Anordnungen zum Vorgehen gegen rechtswidrige Inhalte auf Grundlage des Unionsrechts oder nationalen Rechts erlassen können. Die Bundesnetzagentur wiederum stellt für die Meldung von Verstößen gegen den DSA unter anderem ein Beschwerdeportal bereit.

4.2.7 Feuerwehr

Die Feuerwehr in Deutschland unterliegt den Feuerwehrgesetzen der Bundesländer, die ihre Aufgaben im Brandschutz, der technischen Hilfeleistung und im Katastrophenschutz definieren. Ihre Zuständigkeit erstreckt sich primär auf die Gefahrenabwehr, nicht jedoch auf die Bekämpfung von Falschinformationen. Dennoch kann es Situationen geben, in denen Falschinformationen die Einsatzfähigkeit der Feuerwehr beeinträchtigt, sodass sie in Zusammenarbeit mit anderen Behörden tätig wird.

Die Feuerwehr handelt im Rahmen der Brandschutz-, Rettungsdienst- und Katastrophenschutzgesetze der Länder sowie nach den Feuerwehr-Dienstvorschriften (FwDV). In übergeordneten Fällen kann sie nach Art. 35 GG Amtshilfe leisten und mit Bundesbehörden wie dem THW, dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) oder der Polizei zusammenarbeiten (Dederer 2024 Rn. 52 ff.).

Die Feuerwehr, Ordnungsbehörde und Polizei haben in der Gefahrenabwehr unterschiedliche, aber sich ergänzende Zuständigkeiten. Die Feuerwehr ist primär für die **technische Gefahrenabwehr** zuständig, insbesondere für Brandbekämpfung, Rettungseinsätze und Katastrophenschutz (VG Mainz BeckRS 2020, 37595 Rn. 25 f.). Die Ordnungsbehörden übernehmen die präventive Gefahrenabwehr, indem sie Sicherheitsvorkehrungen durchsetzen, etwa im Baurecht, Umwelt- und Gesundheitsschutz. Die Polizei hingegen ist sowohl für die präventive als auch repressive Gefahrenabwehr verantwortlich, sichert Gefahrenbereiche, unterstützt Evakuierungen und verfolgt Straftaten wie Brandstiftung. In der Praxis arbeiten alle drei Behörden eng zusammen, insbesondere in Katastrophenlagen oder bei Großschadensereignissen, um eine effektive Gefahrenabwehr und den Schutz der Bevölkerung sicherzustellen.

Eine direkte Zuständigkeit zur Bekämpfung von Falschinformationen besteht zwar nicht. Die Feuerwehr kann jedoch bei der Verbreitung von Falschinformationen tätig werden, wenn diese eine **unmittelbare Gefährdung für Menschenleben oder den Bevölkerungsschutz** darstellen. Eine solche Situation kann auftreten, wenn **Gefahrenabwehrmaßnahmen beeinträchtigt** werden, etwa durch gefälschte Notfallmeldungen, die Rettungskräfte zu unnötigen Einsätzen rufen und dadurch Kapazitäten binden. Ebenso kritisch sind gezielte Desinformationen, die verhindern, dass Menschen rechtzeitig evakuiert werden oder lebensrettende Anweisungen ernst nehmen. Zudem können manipulierte Informationen den Bevölkerungsschutz gefährden, wenn beispielsweise falsche Warnungen vor Gaslecks, Bränden oder anderen Gefahren dazu führen, dass Menschen ihre Häuser verlassen oder in gefährliche Gebiete strömen. Solche Falschinformationen können dazu beitragen, dass **Feuerwehrkräfte und andere Einsatzkräfte unnötig alarmiert** werden, während an anderer Stelle dringend Hilfe benötigt wird. In solchen Fällen stimmen sich die Feuerwehr, der Katastrophenschutzstab und die Polizei eng ab, um offizielle Informationen schnell und gezielt an die Bevölkerung weiterzugeben. Zur Verbreitung gesicherter Informationen kann die Feuerwehr-Pressestelle in Kooperation mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) offizielle **Warnmeldungen über das Modulare Warnsystem (MoWaS) oder die NINA-Warn-App** veröffentlichen. Ziel ist die effektive Widerlegung von Falschmeldungen und die Versorgung der Bevölkerung mit verlässlichen, geprüften Informationen.

4.2.8 Technisches Hilfswerk

Das Technische Hilfswerk (THW) ist eine Bundesanstalt und untersteht dem Bundesministerium des Innern und für Heimat (BMI). Seine primäre Aufgabe liegt im Bereich des **Zivil- und Katastrophenschutzes**, wobei es in verschiedenen Einsatzkontexten tätig wird. Der Umgang mit Falschinformationen hängt stark von deren Art und Ursprung ab (§ 1 THWG). Auch wenn das THW keine primäre Zuständigkeit für die Bekämpfung von Falschinformationen hat, kann es in bestimmten Fällen tätig werden. Besonders dann, wenn **Falschinformation Einsätze behindert, Einsatzkräfte gefährdet oder die Bevölkerung verunsichert**, kann das THW im Rahmen seiner gesetzlichen Aufgaben Maßnahmen ergreifen. Laut § 1 Abs. 2 THWG ist das THW für technische Hilfeleistungen im Zivil- und Katastrophenschutz sowie in der Gefahrenabwehr zuständig. **Falschmeldungen über betroffene Gebiete, Bedrohungslagen oder Einsatzmaßnahmen** können den Ablauf von Rettungs- und Hilfsaktionen stören. Daher kann das THW Falschinformationen korrigieren, wenn diese eine unmittelbare Gefahr für die Einsatztätigkeit darstellen.

Ein weiteres wichtiges Element ist die **Zusammenarbeit mit anderen Behörden**, die durch Art. 35 GG sowie § 1 Abs. 1 THWG geregelt ist. Diese Vorschriften verpflichten Bundes- und Landesbehörden zur gegenseitigen Amtshilfe. Das THW arbeitet regelmäßig mit Polizei, Feuerwehr und dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) zusammen. Falls Falschinformationen in einer Katastrophenlage zu Fehlverhalten führen, kann das THW mit den zuständigen Behörden klare und verlässliche Informationen verbreiten, um Gefährdungen zu minimieren. Zur Unterstützung seiner Aufgaben im digitalen Raum verfügt das THW zudem über ein spezialisiertes Virtual Operations Support Team (**VOST**), das als eigene Facheinheit vollständig in die Organisationsstruktur des THW integriert ist (Technisches Hilfswerk). Das VOST übernimmt im Rahmen seiner Zuständigkeit insbesondere die digitale Lageerkundung und -auswertung, etwa durch Social Media Monitoring, Kartierung relevanter Inhalte sowie die Identifikation möglicher Falschinformation. Es wird ausschließlich auf Anforderung tätig und liefert einsatzrelevante Informationen an Führungsstäbe oder Entscheidungsträger:innen, etwa zur Einschätzung der Verbreitungslage oder zur Früherkennung potenziell schädlicher Inhalte. Durch seine Einbindung in die Bundesanstalt ist das VOST rechtlich und organisatorisch Teil der behördlichen Gefahrenabwehrstrukturen und unterstützt damit das THW bei der Bewältigung komplexer Lagen, in denen strategische Kommunikation und Desinformationsbekämpfung eine zentrale Rolle spielen.

Ein weiterer wichtiger Aspekt ist die **Öffentlichkeitsarbeit und Krisenkommunikation**, für die das THW eine eigene Pressestelle unterhält. Diese informiert über Einsätze, Sicherheitsmaßnahmen und richtige Verhaltensweisen in Krisensituationen. Zudem trägt sie zur Richtigstellung falscher Berichte über das THW bei und klärt über Falschinformationen auf, die den Bevölkerungsschutz gefährden könnten. Darüber hinaus ist die Bekämpfung von Desinformation Teil der **nationalen Sicherheitsstrategie**, da Falschinformationen zunehmend als hybride Bedrohung betrachtet werden. Das BMI koordiniert Maßnahmen gegen solche Bedrohungen, und das THW kann als operative Einheit in diesem Rahmen zur Aufklärung und Verbreitung richtiger Informationen beitragen.

Hinsichtlich der Zusammenarbeit des THW und seiner Facheinheit VOST mit anderen Behörden ergeben sich Handlungsspielräume durch den Schutz eigener Einsätze, die Zusammenarbeit mit anderen Behörden, die Öffentlichkeitsarbeit und die Unterstützung nationaler Sicherheitsmaßnahmen. Es agiert als **Partner in einem behördlichen Netzwerk**, wenn Falschinformation konkrete Risiken für Einsätze oder die öffentliche Sicherheit darstellt. Beispielsweise kann es nach einer schweren Überschwemmung vorkommen, dass in sozialen Medien Falschmeldungen über angebliche Evakuierungen verbreitet werden, obwohl keine akute Gefahr besteht. Dies kann Panik auslösen und die Verkehrswege blockieren, wodurch Rettungskräfte behindert werden. In solchen Fällen arbeitet das THW eng mit der örtlichen Feuerwehr, der Polizei und dem Katastrophenschutzstab zusammen, um die Lage zu bewerten und Fehlinformationen zu korrigieren. Die Pressestelle des THW gibt eine offizielle Mitteilung heraus, um die Bevölkerung zu beruhigen und für Klarheit zu sorgen. Zusätzlich kann in Abstimmung mit den zuständigen Behörden eine gezielte Informationskampagne in sozialen Medien gestartet werden, um verlässliche Evakuierungshinweise zu verbreiten und falsche Meldungen zu entkräften.

Die Lösungen zu diesem Quiz finden Sie auf den Seiten 170 f.

Frage 1

Welche Behörde ist vorrangig für die Bekämpfung von staatlich gelenkten Desinformationskampagnen aus dem Ausland zuständig?

a) Die Polizei, da sie für alle Arten der Gefahrenabwehr verantwortlich ist.

b) Das Bundesamt für Verfassungsschutz, da es als „Frühwarnsystem“ für Bedrohungen der demokratischen Ordnung dient.

c) Die Bundesnetzagentur, da sie für die Regulierung digitaler Plattformen zuständig ist.

d) Das BSI, da es für die Cybersicherheit des Bundes zuständig ist.

Frage 2

In welchem Fall könnte eine Ordnungsbehörde gegen die Verbreitung von Desinformation vorgehen?

a) Wenn eine Falschmeldung über eine lokale Veranstaltung verbreitet wird und dadurch die öffentliche Sicherheit und Ordnung gefährdet sein könnte.

b) Wenn eine Privatperson in sozialen Medien über eine andere Person eine unwahre Behauptung aufstellt.

c) Wenn eine (inter-)nationale Desinformationskampagne in sozialen Medien kursiert.

d) Wenn ein Journalist einen Artikel mit fehlerhaften Informationen veröffentlicht.

Frage 3

Welche Behörde ist vorrangig für die Regulierung von Online-Plattformen im Zusammenhang mit Desinformation zuständig?

a) Das BSI, da es für Cybersicherheit verantwortlich ist.

b) Das BKA, da es für Internetkriminalität zuständig ist.

c) Die Bundesnetzagentur, da sie die Umsetzung des Digital Services Act (DSA) in Deutschland koordiniert.

d) Das BfV, da es staatlich gelenkte Desinformation beobachtet.

5. Datenschutzrechtliche Grundlagen

Bei der Vornahme von Maßnahmen gegen Falschinformationen werden Sie sich besonders im digitalen Raum immer wieder mit der Frage konfrontiert sehen, ob Ihr Vorgehen noch **datenschutzkonform** ist. Die in diesem Kapitel vermittelten Grundlagen sollen Ihnen bei einer eigenen Ersteinschätzung helfen. Bei Zweifeln und zur Sicherheit ist der Datenschutz allerdings ein Bereich, bei dem es sich immer lohnt, **Expert:innen zu Rate zu ziehen**.

5.1 Der Personenbezug von Daten

In diesem Kapitel erfahren Sie zum einen, wann überhaupt der **Personenbezug von Daten als notwendige Voraussetzung** der Anwendbarkeit des Datenschutzes gegeben ist. Zum anderen betrachten wir die Maßnahmen der **Anonymisierung und Pseudonymisierung als Hilfsmittel**, um datenschutzkonform agieren zu können.

5.1.1 Wann steht ein Datenschutzverstoß im Raum?

Die **europäische Datenschutzgrundverordnung (DSGVO)** definiert einen Datenschutzverstoß in Art. 4 Nr. 12 DSGVO als einen **Vorfall, bei dem der Schutz personenbezogener Daten verletzt wird**. Dies geschieht, wenn die Sicherheit der Daten gefährdet ist, sei es durch einen Fehler oder durch absichtliches Fehlverhalten. Solche Vorfälle können beispielsweise dazu führen, dass Daten gelöscht, verändert, verloren gehen, unbefugt eingesehen oder weitergegeben werden – unabhängig davon, ob diese Daten übermittelt, gespeichert oder auf andere Weise verarbeitet wurden (DS-GVO-Klabunde/Horváth, Art. 4 Rn. 7 ff.). Damit sind die Handlungen, die einen Datenschutzverstoß bedingen können, **denkbar weit** gehalten. Auch auf ein Verschulden der/des Verantwortlichen, also ein Handeln mit Vorsatz oder Fahrlässigkeit, kommt es nicht an, es reicht allein das **Eintreten des „Verletzungserfolgs“**. Auch bei Einhaltung aller erforderlichen Sicherheitsmaßnahmen kann also ein Verstoß vorliegen, selbst wenn die Offenlegung personenbezogener Daten durch einen Angriff von außen erfolgt.

Verantwortlicher im Sinne der DSGVO ist gem. Art. 4 Nr. 7 „die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet“. Auch dies ist also weit formuliert; verantwortlich können unter den gegebenen Voraussetzungen auch staatliche Behörden und sonstige BOS sein. Darüber hinaus muss die verantwortliche Person sich auch Verletzungen auf Seiten ihrer sog. **Auftragsverarbeiter** zurechnen lassen, also einer natürlichen oder juristischen Person, Behörde, Einrichtung oder anderen Stelle, die personenbezogene Daten im Auftrag der verantwortlichen Person verarbeitet (Art. 4 Nr. 8 DSGVO; DS-GVO-Klabunde/Horváth, Art. 4 Rn. 37 ff.).

Es sollte also ein Anliegen sein, Datenschutzverstöße möglichst zu vermeiden, nicht zuletzt, um nicht zur Zahlung unter Umständen horrender **Bußgelder** verpflichtet zu werden (Art. 83 DSGVO). Selbst bei einem weniger gewichtigen Verstoß stehen potenziell Bußgelder von bis zu 10.000.000 EUR im Raum (Art. 83 Abs. 4 DSGVO). Bei der Verhängung einer Geldbuße und ihrem Betrag werden u. a. die Art, Schwere und Dauer des Verstoßes, das Ausmaß des Schadens, der Grad der Verantwortung für den Verstoß, etwaige einschlägige frühere Verstöße sowie jegliche anderen erschwerenden oder mildernden Umstände im jeweiligen Fall berücksichtigt (Art. 83 Abs. 2 DSGVO).

Das Feld des Datenschutzes bleibt ein umfangreiches und komplexes. Der sachliche Anwendungsbereich ist **weit und einzelfallabhängig**. Auch hinsichtlich der **Regelungsstruktur** kann es schnell unübersichtlich werden. Die DSGVO ist eine europäische Verordnung, welche allein in Deutschland zusätzlich in Kombination mit dem Netzwerkdurchsetzungsgesetz und dem Bundesdatenschutzgesetz, dem Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz, dem Telemediengesetz, Landesdatenschutzgesetzen und sonstigen bereichsspezifischen Datenschutzgesetzen betrachtet werden muss. Aufgaben der Gefahrenabwehr und Strafverfolgung im Rahmen der Bekämpfung von Desinformationen können zudem wiederum den genannten anderweitigen Richtlinien unterfallen. Zusätzlich ist das Problem der Datenverarbeitung im Bereich der Desinformationsbekämpfung und -prävention **nicht auf die nationale Ebene begrenzt**, sodass auch das Zusammenwirken mit nationalen Regelungen weiterer Länder und deren Anwendbarkeit berücksichtigt werden müssen.

Es kann also nötig sein, **bei bzw. vor einer Datenverarbeitung Datenschutzrechtler:innen zurate** zu ziehen. Wann BOS dies konkret tun sollten, lässt sich aufgrund der dargestellten Unübersichtlichkeit datenschutzrechtlicher Anforderungen meist am besten **anhand der Komplexität und Unsicherheit des Falls** entscheiden. Bei einfachen, standardisierten Aufgaben, die klare gesetzliche Regelungen haben, ist das möglicherweise nicht notwendig. Stößt man jedoch auf Unsicherheiten oder sind die rechtlichen Anforderungen unklar, sollte man in jedem Fall eine:n Datenschutzexpert:in zu Rate ziehen. So ist das **Social Media Monitoring** beispielsweise sehr eingriffsintensiv und betrifft den Datenschutz stark. BOS sollten daher **bereits vor Durchführung** der entsprechenden Handlungen ein:e Datenschutzexpert:in zu Rate ziehen und in den weiteren Umsetzungsprozess integrieren. Plant eine Behörde etwa eine Informationskampagne auf ihrer Website, um Bürger:innen über häufige Desinformationen im Zusammenhang mit städtischen Notfalldiensten aufzuklären und greift nur allgemeine Falschinformationen auf, um diese richtigzustellen, ohne konkrete Social Media-Beiträge oder personenbezogene Daten zu nennen, werden in der Regel keine personenbezogene Daten verarbeitet. Es handelt sich um eine standardisierte Maßnahme mit klaren rechtlichen Vorgaben. Ein:e Expert:in sollte hinzugezogen werden, wenn die Maßnahme darüber hinausginge, beispielsweise durch die Analyse oder Veröffentlichung konkreter Nutzendenkommentare oder Social Media-Profile.

5.1.2 Besonderheiten bei Aufgaben der Gefahrenabwehr sowie Strafermittlung und -verfolgung

Relevant für öffentliche Behörden, die mit den Aufgaben der Gefahrenabwehr betraut sind, ist **Art. 2 Abs. 2 DSGVO**: Demzufolge finden die DSGVO und damit ihre Anforderungen keine Anwendung bei der Verarbeitung von personenbezogenen Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit. Dies dürfte einen Großteil der Datenverarbeitung personenbezogener Daten erfassen, die BOS für diverse Maßnahmen gegen Desinformation vollziehen. Im Einzelfall werden BOS dann vielmehr diese **Zweckbindung ihrer Datenverarbeitung** nachweisen müssen.

Der diesbezügliche Datenschutz ist deshalb aber nicht unreguliert, sondern Gegenstand der am 27.4.2016 **parallel mit der DSGVO verabschiedeten Richtlinien** "zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates ((EU) 2016/680)" und "über die Verwendung von Fluggastdaten (PNR Daten) zur Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität ((EU) 206/681)". Diese wurde bisher noch nicht in deutsches Recht umgesetzt.

Die Richtlinie (EU) 2016/680, auch als **Strafverfolgungsrichtlinie** bekannt, regelt die Verarbeitung personenbezogener Daten durch Behörden, die mit der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten sowie der Strafvollstreckung beauftragt sind. Sie schreibt vor, dass solche Datenverarbeitungen auf einer klaren gesetzlichen Grundlage beruhen und an den Zweck der Strafverfolgung oder Gefahrenabwehr gebunden sein müssen. Im Unterschied zur DSGVO können die Rechte der betroffenen Personen – wie das Recht auf Auskunft oder Löschung – eingeschränkt werden, wenn dies aus Gründen der öffentlichen Sicherheit oder zur Verhinderung von Straftaten erforderlich ist. Diese Flexibilität gilt insbesondere dann, wenn eine Einwilligung der Betroffenen nicht eingeholt werden kann, und **ermöglicht es Behörden, Daten auch ohne deren Zustimmung zu nutzen**. Gleichzeitig fordert die Richtlinie, dass die Verarbeitung **verhältnismäßig** bleibt und **Sicherheitsmaßnahmen** wie Verschlüsselung oder Zugriffsbeschränkungen eingehalten werden.

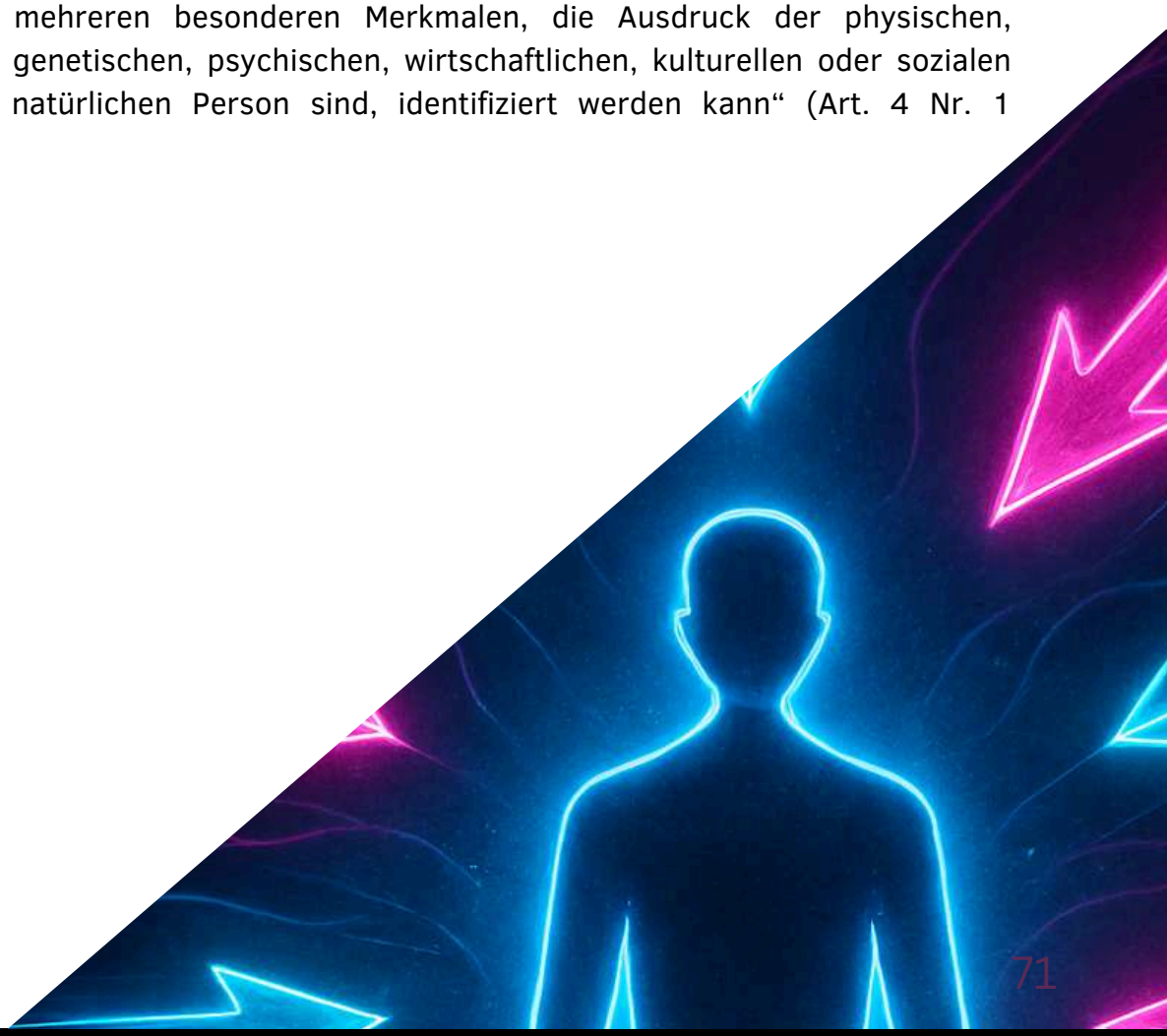
Die Strafverfolgungsrichtlinie erlaubt den Behörden eine flexiblere und umfassendere Verarbeitung personenbezogener Daten als die DSGVO. Dies betrifft insbesondere die automatisierte Datenverarbeitung und die längeren Speicherfristen. Nichtsdestotrotz müssen Behörden Eingriffe in die Grundrechte der Betroffenen verhältnismäßig gestalten. Die Abweichungen von der DSGVO verdeutlichen den Versuch, eine Balance zwischen den **Erfordernissen der Strafverfolgung und Gefahrenabwehr** einerseits und dem **Schutz der Privatsphäre** andererseits zu schaffen.

5.1.3 Dreh- und Angelpunkt: Der Personenbezug von Daten

Da eine Vielzahl an Verarbeitungsvarianten einen Datenschutzverstoß darstellen können – im Kampf gegen Desinformationen etwa auch das Teilen bildlicher Inhalte zur Entkräftung –, ist ein erster Punkt, den BOS aufmerksam beachten sollten, ob die verarbeiteten Daten einen **Personenbezug** besitzen. Sollte dem nicht so sein, wäre bereits die Grundvoraussetzung eines Datenschutzverstoßes nicht erfüllt. Wichtig: Der Personenbezug von Daten ist zwar eine notwendige, **nicht jedoch die alleinige Voraussetzung** der Anwendbarkeit der DSGVO (siehe Art. 2 DSGVO).

Der Europäische Gerichtshof entschied 2023, dass die Kategorisierung als personenbezogenes Datum **weit auszulegen** ist (EuG, Urteil vom 26.4.2023 – T-557/20). Sie ist nicht auf sensible oder private Informationen beschränkt, sondern umfasst **potenziell alle Arten von Informationen** sowohl objektiver als auch subjektiver Natur in Form von Stellungnahmen oder Beurteilungen. Voraussetzung ist, dass es sich um Informationen "**über" die in Rede stehende Person** handelt, also um eine Information, die aus Sicht der Empfangenden der Datenübermittlung auf Grund ihres Inhalts, ihres Zwecks oder ihrer Auswirkungen mit einer bestimmten Person verknüpft ist. Auch persönliche Sichtweisen oder Meinungen, welche zur Entkräftung von Desinformationen geteilt werden, können damit potenziell personenbezogene Daten im Sinne der DSGVO darstellen.

Was ist nun aber dieser "Personenbezug"? **Art. 4 Nr. 1 DSGVO** definiert personenbezogene Daten als "alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person [...] beziehen". Natürliche Personen sind also nicht etwa andere Behörden oder Unternehmen, sondern der/die Einzelne. **"Identifizierbar"** wiederum ist ein relativ vager und breiter Begriff. Eine Person ist dann identifizierbar, wenn sie "direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann" (Art. 4 Nr. 1 DSGVO).



Eine umfangreiche Liste also, unter die nach Rechtsprechung des Europäischen Gerichtshofs nicht nur Daten wie Benutzername und Passwörter, sondern auch vom Betroffenen während des Webbrowsing erfasste Daten, z. B. sog. Cookies fallen (EuGH Urt. v. 1.10.2019 – C- 673/17). Cookies können nämlich durch die Verknüpfung mit anderen Daten des sonstigen Verhaltens einer Person im Internet (z. B. einer IP-Adresse oder einem Benutzendenkonto) zu ihrer **Identifizierung** führen. Auch Standortdaten können darüber hinaus personenbezogen sein. Der Begriff selbst wird in der DSGVO zwar nicht ausdrücklich definiert, ist aber in sinnvoller rechtseinheitlicher Interpretation als eine Abfolge von Feststellungen von geographischem Ort und Zeitpunkt eines Gerätes bzw. einer Person zu verstehen (DS-GVO-Klabunde/Horváth, Art. 4 Rn. 16).

Bei einer möglichen **Social Media Analyse** im Kampf gegen Desinformationen kann eine Behörde sich also schnell im Rahmen eines potenziellen Datenschutzverstoßes bewegen. Auch wenn Social Media Profile keine Klarnamen enthalten, besteht bei einer Datenverarbeitung häufig ein Personenbezug. So könnten mit Standortdaten personenbezogene Daten im Sinne der DSGVO verarbeitet werden. Auch Datensätze, die aus IP-Adressen und Zeitangaben bestehen oder sonstige technische Kennungen von Kommunikationsgeräten beinhalten, können Rückschlüsse auf die Betroffenen erlauben und haben damit Personenbezug. In der Folge müssen BOS dabei die Anforderungen der DSGVO beachten.

Diese Identifizierung muss auch nicht die Behörde als verantwortliche Instanz selbst durchführen können. Es reicht, dass **irgendein Dritter** nach allgemeinem Ermessen diese wahrscheinlich durchführen kann (DSGVO, EG 26). BOS müssen also nicht nur ihre eigenen Möglichkeiten zur Datenanalyse berücksichtigen, sondern auch die **Möglichkeiten spezialisierter Dritter** wie etwa entsprechender Unternehmen, unabhängig davon, ob sie hierzu beauftragt wurden oder nicht. Ein analoges Beispiel hierfür ist etwa die Verkehrsüberwachung durch staatliche Behörden: Eine staatliche Verkehrsbehörde betreibt ein Netz von Verkehrskameras zur Überwachung des Straßenverkehrs und zur Erkennung von Verkehrsverstößen, welche u. a. das Fahrzeugkennzeichen sowie Bilder des Fahrzeugs und möglicherweise anderer Verkehrsteilnehmer erfassen. Die Verkehrsbehörde verarbeitet die Daten primär für ihre Aufgaben, etwa die Verfolgung von Verkehrsdelikten. Sie kann Kennzeichen auslesen und mit einer Halterdatenbank verknüpfen und Aufnahmen speichern, ohne aber selbst alle abgebildeten Personen oder Fahrzeuge identifizieren zu können. Ein spezialisiertes Unternehmen könnte jedoch z.B. mithilfe von Gesichtserkennungssoftware Personen auf den Aufnahmen identifizieren, wenn Bilder von ihnen (z. B. aus sozialen Netzwerken) in einer externen Datenbank vorliegen. Die Verkehrsbehörde ist zwar für die ursprüngliche Datenverarbeitung verantwortlich, hat aber keinen direkten Einfluss darauf, was Dritte mit den Daten machen könnten.

Trotzdem muss sie diese Möglichkeiten bei der Erfassung und Speicherung der Daten berücksichtigen, und muss sicherstellen, dass ihre eigene Erhebung und Verarbeitung der Daten den Datenschutzanforderungen genügt. Dies schließt ein, die potenziellen Risiken der Identifizierung durch Dritte zu bewerten und **Maßnahmen zum Schutz der betroffenen Personen** zu ergreifen (z.B. Anonymisierung oder strenge Zugriffsbeschränkungen).

5.1.4 Pseudonymisierung vs. Anonymisierung

Wichtig bei der Frage, ob man den Personenbezug vermeiden kann, ist die Differenzierung zwischen **”Pseudonymisierung“** und **”Anonymisierung“**. Pseudonymisierung bezeichnet die Verarbeitung personenbezogener Daten in einer Weise, dass diese ohne Hinzuziehen zusätzlicher Informationen nicht mehr einer spezifischen Person zugeordnet werden können. Dazu werden diese zusätzlichen Informationen gesondert aufbewahrt und unterliegen technischen und organisatorischen Maßnahmen, die das gewährleisten (Art. 4 Nr. 5 DSGVO). Es handelt sich letztendlich lediglich um eine **andere Form der Speicherung**, wobei den Verantwortlichen weiterhin der **vollständige Informationsgehalt der Daten** zur Verfügung steht und der individuelle Bezug jedes Informationselements ohne großen Aufwand hergestellt werden kann. Die Pseudonymisierung bietet somit im Gegensatz zur Anonymisierung **keinen vollständigen Schutz der Privatsphäre**, da die Datenverantwortlichen den Personenbezug wiederherstellen können (DS-GVO/BDSG-Hansen, Art. 4 Nr. 5 Rn. 13 ff.). Eine bloße Verschlüsselung von Daten birgt das gleiche Problem. Verschlüsselte Speicherung und Übertragung sind zwar Sicherheitsmaßnahmen, stehen einer Identifizierbarkeit der betroffenen Person jedoch nicht hinreichend im Weg.

Bei einer **echten Anonymisierung** werden hingegen die personenbezogenen Daten unmittelbar so verändert, dass die **Identifizierbarkeit der betroffenen Personen nicht mehr gegeben** ist (DS-GVO/BDSG-Hansen, Art. 4 Nr. 5 Rn. 13 ff.). Hierfür gibt die DSGVO kein Verfahren vor. Vielmehr muss der oder die Verantwortliche wiederum überprüfen, ob die Daten im Ergebnis den in der DSGVO dargestellten Personenbezug weiterhin vorweisen. Dies ist selten zweifelsfrei festzustellen; gerade Standortdaten können hierfür eine große Herausforderung darstellen. Es ist zudem fraglich, ob ein so hoher Grad an Anonymisierung bei der Bekämpfung von schnell verbreiteten Desinformationen und Desinformationskampagnen inhaltlich sinnvoll und praktisch umsetzbar ist. Solche Maßnahmen könnten die **Effektivität und Handhabbarkeit** von Gegenmaßnahmen einschränken. Im Ergebnis müssen BOS also abwägen, ob es zielführender und im Einzelfall effektiv ist, das Werkzeug der Anonymisierung zu nutzen, um möglichst von vornherein nicht dem Datenschutz zu unterliegen, oder ob es sich mehr lohnt, einen bestehenden Personenbezug von Daten hinzunehmen und sich in der Folge an die entsprechenden rechtlichen Anforderungen halten zu müssen.

5.2 Ein Überblick über mögliche datenschutzrechtliche Rechtsgrundlagen

Wenn die Voraussetzungen der Anwendbarkeit der DSGVO vorliegen, bedeutet das nicht direkt, dass auch ein Datenschutzverstoß vorliegt. Vielmehr müssen dann bei der Datenverarbeitung die **Anforderungen der DSGVO** (und weiterer deutscher Datenschutzgesetze) beachtet werden. Unter anderem gehört hierzu die Verarbeitung aufgrund einer **gesetzlichen Ermächtigung**. Bei behördlicher Datenverarbeitung im Rahmen des Vorgehens gegen Desinformationen kommen folgende Rechtsgrundlagen in Betracht: Die Einwilligung der betroffenen Person (Art. 6 Abs. 1 lit. a DSGVO) oder das „öffentliche Interesse“ der Behörde oder öffentlicher Stellen (Art. 6 Abs. 1 lit. e DSGVO). Darüber hinaus sind die aus Art. 2 Abs. 2 DSGVO folgenden Ausnahmen zu beachten. Demnach gilt die DSGVO nicht für Verarbeitungen personenbezogener Daten, die unter anderem im Rahmen von Tätigkeiten erfolgen, die nicht dem EU-Recht unterliegen, wie beispielsweise der Strafverfolgung, der nationalen Sicherheit oder der Gefahrenabwehr. Hierbei greifen speziellere europäische Richtlinien (siehe Kapitel 5.1.1).

5.2.1 Suche nach der passenden Rechtsgrundlage

Bei der Verarbeitung von personenbezogenen Inhalten in der Öffentlichkeitsarbeit müssen BOS die **geeigneten Rechtsgrundlagen** auswählen, um sowohl die Interessen der betroffenen Personen als auch die Interessen der eigenen Organisation angemessen zu berücksichtigen. Bei dieser Verarbeitung können außerdem **Grundrechte** betroffen sein. In diesen Fällen ist es wichtig, dass solche Eingriffe immer auf einer **klaren gesetzlichen Grundlage** basieren (Hamann et al. 2023, § 8 Rn. 606 f.). Entsprechend dem **Grundsatz der Zweckbindung** der DSGVO stellt hierbei jede Zweckänderung hinsichtlich der Datenverarbeitung – etwa Daten, die zunächst zu Strafverfolgung erhoben wurden und anschließend für präventive Polizeiarbeit genutzt werden sollen – einen neuen Grundrechtseingriff dar und bedarf neuer Legitimation und somit auch einer neuen Ermächtigungsgrundlage (DS-GVO BDSG-Pötters, Art. 5 Rn. 13 ff.). Ähnlich gilt dies bei der **Datenüberführung** bspw. von der Polizei an die Staatsanwaltschaft, sollte eine strafrechtliche Relevanz desinformierender Inhalte im Raum stehen: Sowohl die damit einhergehende mögliche Zweckänderung oder jedenfalls der Akt der Übermittlung als auch die Weiterverarbeitung der Daten stellen eigenständige Grundrechtseingriffe dar, die grundsätzlich jeweils einer eigenen Ermächtigungsgrundlage bedürfen. Im Einzelfall kann dies der Gesetzgeber bereits bedacht und eine Ermächtigungsgrundlage erlassen haben, die beide Maßnahmen als eine Form **”einheitlicher Überführungsermächtigung“** abdeckt.

Ein Beispiel hierfür ist § 481 Abs. 1 S. 1 StPO: Das Gesetz erlaubt die Übermittlung personenbezogener Daten, die aus einem Strafverfahren stammen, an die Polizeibehörde zum Zwecke der weiteren Datenverarbeitung nach Maßgabe der Polizeigesetze (Roggenkamp 2019 Rn. 70). Die Zulässigkeit der gewählten Rechtsgrundlage muss für jeden **konkreten Fall** geprüft werden, wobei die Verhältnismäßigkeit und das öffentliche Interesse berücksichtigt werden sollten.

5.2.2 Das öffentliche Interesse/die Ausübung öffentlicher Gewalt als Rechtsgrundlage gem. Art. 6 Abs. 1 lit. e DSGVO

Die Öffentlichkeitsarbeit staatlicher Einrichtungen als Maßnahme gegen Falschinformationen kann im **"öffentlichen Interesse" oder in "Ausübung öffentlicher Gewalt"** gem. Art. 6 Abs. 1 lit. e DSGVO liegen. Dieses öffentliche Interesse stellt allerdings **keine eigenständige Ermächtigungsgrundlage** für die Datenverarbeitung dar. Es bedarf einer konkreten Grundlage im Unionsrecht oder im Recht eines Mitgliedsstaates (Erwägungsgrund 45 der DSGVO). Eine solche hat Deutschland mit **§ 3 BDSG (Bundesdatenschutzgesetz)** geschaffen. Die Regelungen konzentrieren sich auf die Wahrnehmung im öffentlichen Interesse liegender Aufgaben oder solcher, die in Ausübung hoheitlicher Gewalt erfolgen. Hierzu zählen auch sämtliche **Bereiche der Ordnungsverwaltung**, also solche Tätigkeiten, die der Aufrechterhaltung der öffentlichen Ordnung und Sicherheit dienen, z.B. Polizei- und Strafverfolgungsmaßnahmen. Auch wenn private Organisationen im Auftrag einer öffentlichen Behörde Aufgaben übernehmen, fallen diese privaten Organisationen unter diese Regelungen. Im Rahmen ihrer Tätigkeit müssen BOS in jedem Einzelfall prüfen, ob und in welchem Umfang der Personenbezug der jeweiligen Mitteilung gemäß Art. 6 Abs. 1 lit. e DSGVO erforderlich ist, um eine Aufgabe im öffentlichen Interesse zu erfüllen oder hoheitliche Gewalt auszuüben (Kühling/Buchner-Buchner/Petri, Art. 6 Rn. 111). Dabei müssen sie sicherstellen, dass die Verarbeitung nicht nur **geeignet und erforderlich**, sondern auch **verhältnismäßig im Hinblick auf die jeweilige Zielsetzung** ist.

Die Relevanz von Art. 6 Abs. 1 lit. e DSGVO als Rechtsgrundlage ist direkt mit dem Anwendungsbereich der DSGVO verknüpft, der in **Art. 2 Abs. 2 DSGVO** geregelt ist (DS-GVO BDSG-Schulz, Art. 6 Rn. 51). Die DSGVO gilt nicht für Verarbeitungen personenbezogener Daten, die unter anderem im Rahmen von Tätigkeiten erfolgen, die nicht dem EU-Recht unterliegen, wie beispielsweise der Strafverfolgung, der nationalen Sicherheit oder der Gefahrenabwehr (Art. 2 Abs. 2 lit. d DSGVO). In solchen Fällen greifen stattdessen die Vorgaben der Richtlinie (EU) 2016/680 oder nationale Regelungen.

Für BOS bedeutet das, dass Art. 6 Abs. 1 lit. e DSGVO als Rechtsgrundlage nur relevant ist, wenn personenbezogene Daten im öffentlichen Interesse oder zur Wahrnehmung hoheitlicher Aufgaben verarbeitet werden, die nicht explizit in den Ausnahmen des Art. 2 Abs. 2 DSGVO genannt sind. Ein Beispiel wäre die Analyse von Falschinformationen zur Förderung von Transparenz und der Stärkung demokratischer Prozesse. Sind jedoch Maßnahmen der Strafverfolgung oder Gefahrenabwehr betroffen, fällt die Verarbeitung aus dem Anwendungsbereich der DSGVO heraus. In solchen Fällen müssen die **spezifischen Anforderungen der einschlägigen Richtlinie oder nationaler Gesetze** beachtet werden.

Daher ist für BOS eine genaue Prüfung im Einzelfall unerlässlich, um festzustellen, ob A**rt. 6 Abs. 1 lit. e DSGVO oder andere rechtliche Regelungen anwendbar sind.**

5.2.3 Einwilligung als Rechtsgrundlage gem. Art. 6 Abs. 1 lit. a DSGVO

Eine weitere Option zur Legitimierung einer Verarbeitung personenbezogener Daten ist die **Einwilligung der betroffenen Person** (siehe Art. 4 Nr. 11, 6 Abs. 1 lit. a, 7 DSGVO). Relevant im Rahmen von Maßnahmen gegen Desinformationen wird dies vor allem bei **presserechtlichen Darstellungen** sein, etwa wenn eine BOS sich entschließt, die Auswirkungen bestimmter Falschinformationen in einem öffentlichen Bericht oder auf ihrer Website darzustellen, um die Öffentlichkeit aufzuklären. Selten wird eine Einwilligung unmittelbar von den Verbreitenden von Desinformation eingeholt werden können, entweder mangels faktischer Umsetzbarkeit oder Sinnhaftigkeit im spezifischen Fall, wäre die Person auf diese Art doch vorab über mögliche Maßnahmen informiert und würde sie einer solchen Verarbeitung doch ohnehin kaum zustimmen.

Die **Einwilligungserklärung** muss transparent, verständlich und klar formuliert sein, damit die betroffene Person alle relevanten Informationen leicht erfassen kann (Art. 7 Abs. 2 DSGVO). Sie muss freiwillig abgegeben werden, ohne dass Nachteile entstehen, wenn sie verweigert oder widerrufen wird (Art. 4 Nr. 11 DSGVO). Die betroffene Person muss vollständig informiert sein, insbesondere über die Datenverarbeitung und mögliche Risiken (Art. 4 Nr. 11 DSGVO). Zudem muss die Einwilligung jederzeit **widerrufbar** sein (Art. 7 Abs. 3 DSGVO). Der Zweck der Datenverarbeitung muss klar und konkret definiert sein (Art. 6 Abs. 1 Buchst. a, Art. 5 Abs. 1 Buchst. b DSGVO), und es muss unmissverständlich eine aktive, bestätigende Handlung der betroffenen Person erfolgen, etwa durch Unterschrift (Art. 4 Nr. 11 DSGVO).

5.3 Die Grundsätze des Datenschutzes

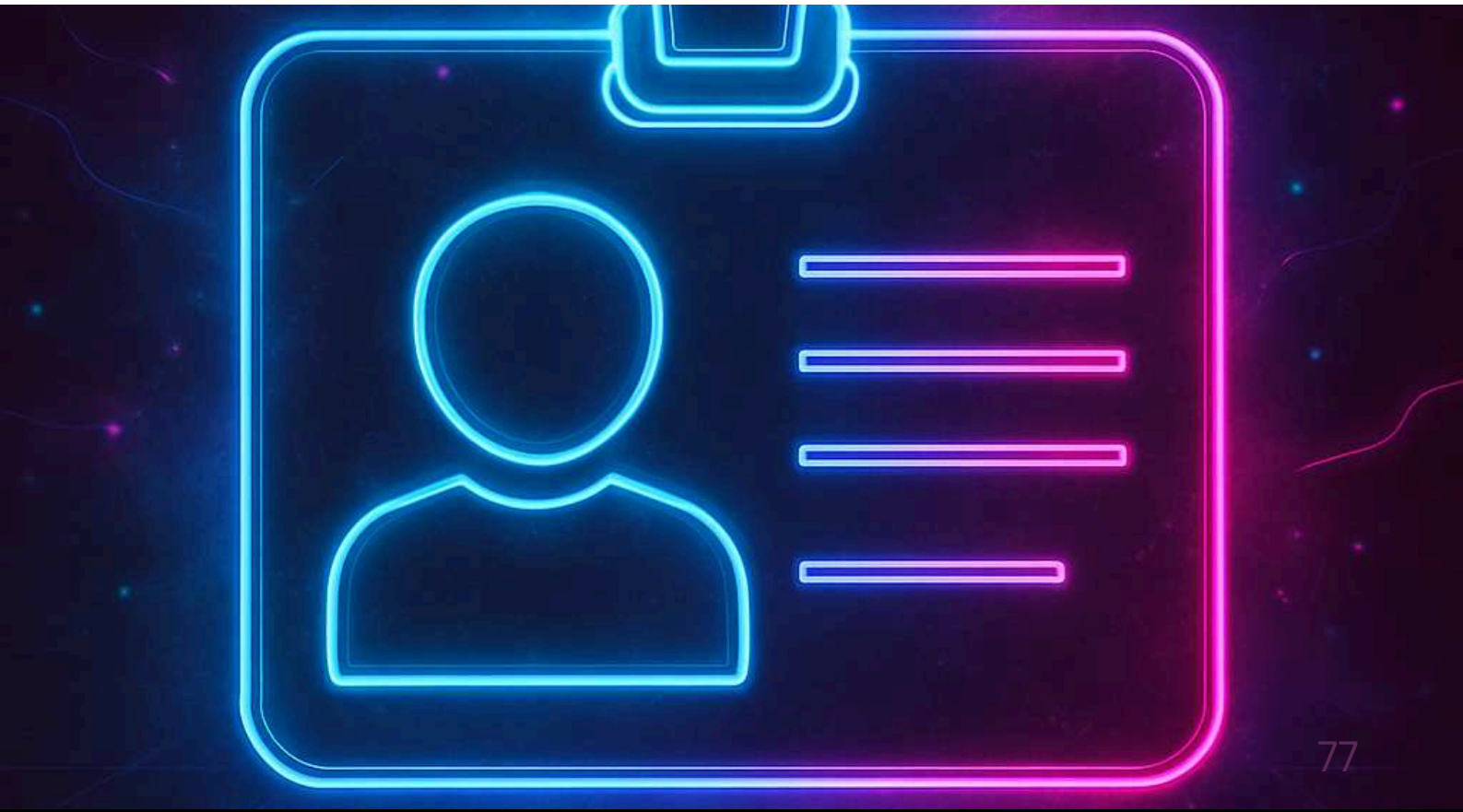
Neben spezifischen Anforderungen diverser Rechtsgrundlagen fordert der Datenschutz die **Einhaltung allgemeiner Grundsätze**, geregelt in **Art. 5 DSGVO**. Diese werden Ihnen im Folgenden übersichtsartig ebenso dargestellt wie Möglichkeiten der Einhaltung derselben.

5.3.1 Rechtmäßigkeit, Treu und Glauben und Transparenz (Abs. 1 lit. a)

Personenbezogene Daten müssen auf **rechtmäßige Weise, fair und transparent** verarbeitet werden. Um ersteres zu erfüllen, bedarf es mindestens einer **hinreichenden Rechtsgrundlage** für die Verarbeitung.

Eine **faire Verarbeitung** entsprechend dem Grundsatz von Treu und Glauben setzt voraus, dass betroffene Personen in der Lage sind, das Vorhandensein einer Verarbeitung zu erfahren und ordnungsgemäß und umfassend über die Bedingungen der Erhebung informiert zu werden (EG 38). Im Ergebnis soll ein Kräftegleichgewicht zwischen betroffener Person und verantwortlicher Stelle ermöglicht werden.

Der **Grundsatz der Transparenz** erfasst den Ausschluss heimlicher Verarbeitungen personenbezogener Daten und die umfassende Information der betroffenen Person über die Verarbeitung der auf sie bezogenen Daten.



5.3.2 Zweckbindung (Abs. 1 lit. b)

Personenbezogene Daten dürfen nur für **festgelegte, eindeutige und legitime Zwecke** erhoben und verarbeitet werden. Diese müssen schon bei der Erhebung der Daten festgelegt werden. Der festgelegte Zweck bestimmt dann etwa, welche Daten verarbeitet und wie lange sie gespeichert werden dürfen. Hieraus ergeben sich die in Abschnitt 2.2 (siehe Kapitel 5.2.1) genannten Probleme einer Zweckänderung infolge der Zusammenarbeit von Behörden im Kampf gegen Falschinformationen.

5.3.3 Datenminimierung (Abs. 1 lit. c)

Ergänzend zum Zweckbindungsgrundsatz sollten nur die für den jeweiligen Verarbeitungszweck ***erforderlichen*** **personenbezogenen Daten** erhoben und verarbeitet werden. Die Daten müssen für den Zweck angemessen, erheblich und auf das notwendige Maß beschränkt sein.

5.3.4 Richtigkeit (Abs. 1 lit. d)

Die Daten müssen **korrekt und auf dem neuesten Stand** gehalten werden. **“Sachlich richtig“** ist objektiv bewertbar und bedeutet, dass die gespeicherten Informationen mit der Realität übereinstimmen. Inwiefern die Daten auf dem neuesten Stand gehalten werden müssen, hängt von dem verbundenen Zweck ab. Beispielsweise beziehen sich Daten über den Gesundheitszustand der betroffenen Person, die bei einer bestimmten Untersuchung gewonnen wurden, selbstverständlich nur auf den Zeitpunkt dieser Untersuchung. Wenn jedoch der Verdacht eines strafbaren Verhaltens bei der Verbreitung oder Veröffentlichung von Falschinformationen, bspw. Verleumdungen oder Volksverhetzung, später entkräftet wird, etwa durch ein gerichtliches Urteil, müssen die **betroffenen Daten aktualisiert oder gelöscht** werden, um der Unschuld der Person gerecht zu werden und sicherzustellen, dass falsche Verdächtigungen nicht weiterhin zu ihrem Nachteil in den Datenbanken verbleiben (DS-GVO BDSG-Pötters, Art. 5 Rn. 25).

5.3.5 Speicherbegrenzung (Abs. 1 lit. e)

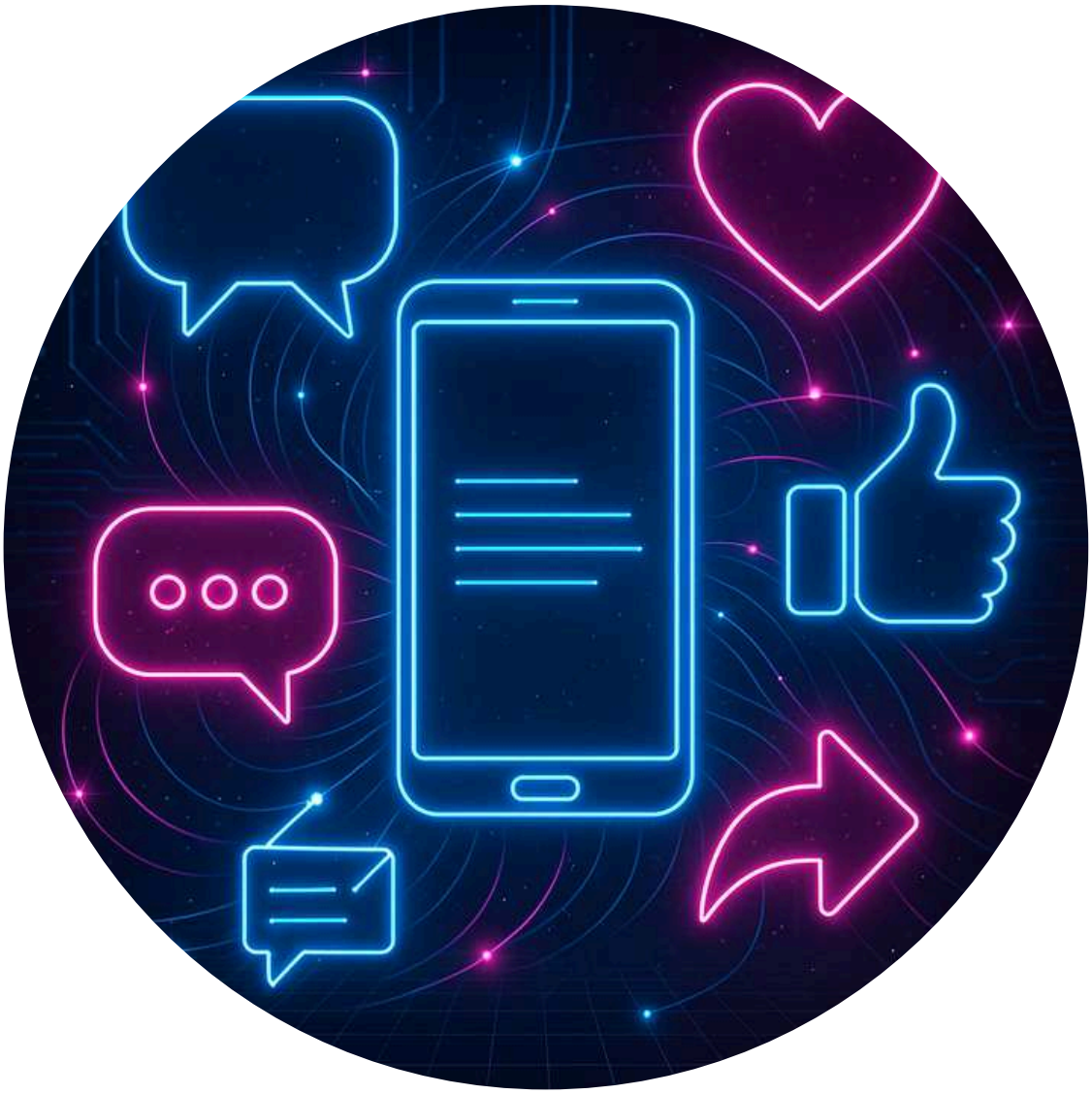
Daten dürfen nur so lange aufbewahrt werden, **wie es für den Verarbeitungszweck erforderlich ist**. Entweder werden personenbezogene Daten nach Erforderlichkeit einer Speicherung gelöscht oder ihr Bezug zur betroffenen Person aufgehoben. Ausnahmen, welche im Rahmen von Falschinformationsbekämpfung relevant sein können, sind solche der **Verarbeitung für Forschungs- und statistische Zwecke** (DS-GVO-Heberlein, Art. 5 Rn. 35). Eine Behörde könnte beispielsweise Falschinformationen sammeln und analysieren, um besser zu verstehen, wie Fehlinformationen die öffentliche Wahrnehmung und Verhaltensweisen beeinflussen. Solche Daten können zu statistischen Zwecken verarbeitet werden, um Muster zu erkennen und künftige Falschinformationen zu verhindern. Sie dürften deshalb auch grundsätzlich länger gespeichert werden, auch wenn sie nicht mehr mit dem ursprünglichen Zweck in Verbindung stehen.

5.3.6 Integrität und Vertraulichkeit (Abs. 1 lit. f)

Es müssen angemessene Sicherheitsmaßnahmen ergriffen werden, um die Daten vor **unbefugtem Zugriff, unrechtmäßiger Verarbeitung und Verlust** zu schützen.

5.3.7 Rechenschaftspflicht (Abs. 2)

Die Verantwortlichen müssen **nachweisen** können, dass sie die Datenschutzgrundsätze einhalten. Dies ist besonders relevant bei einer Überprüfung durch die Aufsichtsbehörden, welche die Befugnis haben, die Verantwortlichen zur Bereitstellung von Informationen anzuweisen.



Die Lösungen zu den folgenden praktischen Übungen finden Sie auf den Seiten 172 ff.

Fallbeispiel 1

Eine Polizeibehörde plant, Social Media-Plattformen nach Kommentaren zu durchforsten, die Desinformationen zu öffentlichen Sicherheitsmaßnahmen enthalten. Ziel ist es, frühzeitig Falschmeldungen zu erkennen, die Panik auslösen oder das Vertrauen in behördliche Maßnahmen untergraben könnten. Hierzu sammelt und analysiert die Polizeibehörde automatisiert Kommentare. Die zuständigen Mitarbeitenden sind der Ansicht, dass die erhobenen Daten keinen Personenbezug haben, da keine direkten Namen oder E-Mail-Adressen erfasst werden. Es werden lediglich die Inhalte der Kommentare und allgemeine Informationen zur Plattform gespeichert.

1. Inwiefern liegt bei den gesammelten Kommentaren ein Personenbezug gemäß Art. 4 Nr. 1 DSGVO vor?

2. Ist eine Identifizierung der Verfassenden der Kommentare durch Kombination mit weiteren Daten möglich?

3. Welche Maßnahmen könnten ergriffen werden, um den Personenbezug zu vermeiden oder zu reduzieren?

Fallbeispiel 2

Eine Polizeibehörde möchte im Rahmen ihrer Öffentlichkeitsarbeit gegen Desinformation eine Kampagne auf Social Media starten. Ziel der Kampagne ist es, Falschmeldungen zu widerlegen, die das Vertrauen der Bevölkerung in staatliche Institutionen untergraben. Dazu sollen gezielt Social Media-Beiträge mit Desinformationen analysiert und richtiggestellt werden. Die Behörde plant, in ihren Veröffentlichungen die Inhalte von Falschmeldungen zu nennen und dabei gegebenenfalls Nutzendenkommentare oder Profilnamen zu verwenden, um die Glaubwürdigkeit ihrer Richtigstellungen zu erhöhen. Unter welchen rechtlichen Voraussetzungen darf die Behörde personenbezogene Daten im Rahmen ihrer Öffentlichkeitsarbeit verarbeiten, und welche gesetzlichen Grundlagen sind dabei zu beachten?

Die Lösungen zu diesem Quiz finden Sie auf den Seiten 174 f.

Frage 1

Welche der folgenden Aussagen beschreibt korrekt den Umgang mit personenbezogenen Daten bei der Weiterverarbeitung in der Öffentlichkeitsarbeit von Behörden?

a) Eine Zweckänderung der Datenverarbeitung, wie die Nutzung von ursprünglich für Strafverfolgung erhobenen Daten für präventive Polizeiarbeit, bedarf keiner neuen Ermächtigungsgrundlage, solange die betroffenen Personen informiert wurden.

b) Die Übermittlung personenbezogener Daten von der Polizei an die Staatsanwaltschaft im Kontext einer strafrechtlichen Relevanz stellt einen eigenständigen Grundrechtseingriff dar, der grundsätzlich einer eigenen Ermächtigungsgrundlage bedarf.

c) Die DSGVO erlaubt jede Zweckänderung der Datenverarbeitung, solange diese im öffentlichen Interesse liegt, ohne dass eine neue rechtliche Grundlage erforderlich ist.

Frage 2

Welche der folgenden Aussagen beschreibt korrekt den “Personenbezug“ von Daten im Sinne der DSGVO?

a) Ein Personenbezug besteht nur, wenn die Daten direkt auf eine Einzelperson wie Name oder Adresse verweisen, ohne dass zusätzliche Informationen erforderlich sind.

b) Auch Standortdaten und technische Kennungen wie IP-Adressen können als personenbezogene Daten gelten, wenn sie mit anderen Informationen verknüpft werden können, die eine Identifizierung der betroffenen Person ermöglichen.

c) Personenbezogene Daten umfassen nur sensible oder private Informationen und schließen keine öffentlich zugänglichen Informationen wie Social-Media-Posts ein.

Frage 3

Im Rahmen einer Social Media Monitoring-Strategie zur Bekämpfung von Desinformationen verwendet eine Behörde IP-Adressen und Zeitstempel (also die genaue Uhrzeit und das Datum, zu denen bestimmte Aktionen im Zusammenhang mit einem Social Media-Account erfolgen), um mögliche Fake-Accounts zu identifizieren. Welche der folgenden Aussagen trifft in Bezug auf die DSGVO am besten zu?

a) IP-Adressen und Zeitstempel sind personenbezogene Daten, da sie unter Berücksichtigung zusätzlicher Informationen zur Identifizierung einer Person verwendet werden können, auch wenn diese nicht unmittelbar durch die Behörde erfolgt.

b) Da IP-Adressen und Zeitstempel allein keine direkte Identifizierung einer Person ermöglichen, unterliegt diese Datenverarbeitung nicht den Anforderungen der DSGVO.

c) Die Verarbeitung dieser Daten ist nur dann datenschutzrechtlich relevant, wenn die Behörde die Absicht hat, eine konkrete Person zu identifizieren.

6. Überblick über Maßnahmen gegen Falschinformationen

6.1 Einführung

BOS haben verschiedene Möglichkeiten, um Falschinformationen etwas entgegenzusetzen. Der folgende Abschnitt gibt Ihnen einen Überblick, welche Maßnahmen BOS gegen Falschinformationen ergreifen könnten. Er basiert auf den im Projekt PREVENT durchgeführten Literaturstudien sowie empirischen Arbeiten.

Wir gliedern diese Gegenmaßnahmen nach verschiedenen Tätigkeiten, die die BOS in Bezug auf Falschinformationen ergreifen können:

- BOS können versuchen, die **Nutzenden von Social Media** aufzuklären und gegen Falschinformationen zu stärken (siehe Kapitel 7)

    - BOS können sich selbst vorbereiten und sich selbst stärken ("**Preparedness**"),
    - indem sie Falschinformationen erkennen und bewerten,
    - indem sie interne Prozesse der Falschinformationsbekämpfung optimieren
    - und indem sie ihre eigenen Mitarbeitenden schulen.

- BOS können Falschinformationen durch eine passende **Kommunikation** eindämmen,
    - indem sie selbst **aktiv und präventiv** gut geprüfte Informationen veröffentlichen,
    - indem sie bereits kursierende Falschinformationen korrigieren (**Debunking**) (siehe Kapitel 9)
    - und indem sie sich aktiv darum bemühen, **Follower:innen** zu gewinnen und zu halten (siehe Kapitel 10).

- BOS können durch **Kooperationen mit anderen Institutionen** – wie anderen BOS, Kommunen, Plattformbetreiber sowie Nichtregierungsorganisationen (NGOs; z.B. Fact-Checking-Organisationen) – ihre Aktivitäten besser koordinieren und durch gegenseitige Hilfe eventuell Ressourcen sparen.

- BOS können auch **eskalieren**,
    - indem sie Falschinformationen an Plattformbetreiber und/oder an Strafverfolgungsbehörden melden,
    - oder indem sie auf ihren eigenen Kanälen Nutzende blockieren oder Posts verbergen oder löschen (siehe Kapitel 11).

- Schließlich können BOS angesichts der Flut an Falschinformationen auch Programme, KI oder Chatbots nutzen, um **automatisiert** gegen Falschinformationen vorzugehen. Dies können sie beim Social Media Monitoring, bei der Informationsweitergabe und Interaktion mit Bürger:innen sowie bei Bekämpfungsmaßnahmen (Debunking, Meldungen, Löschen und Blockieren) einsetzen (siehe Kapitel 12).

Hier ein Überblick über die möglichen Gegenmaßnahmen:

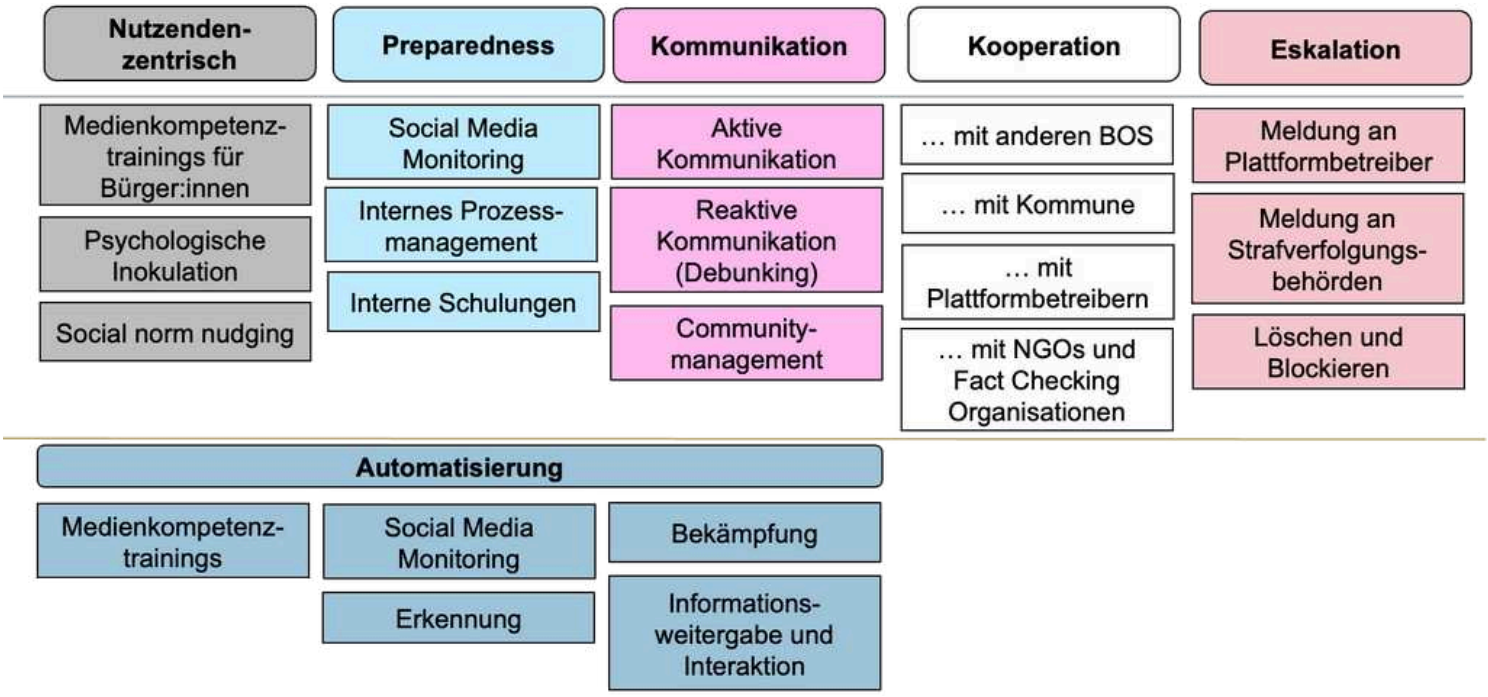


Abbildung 2: (Potentielle) Maßnahmen von BOS gegen Falschinformationen
Quelle: Eigene Darstellung

6.2 Zielgruppen

Die Maßnahmen beziehen sich auf drei Zielgruppen:

1. Aufklärungs- und Stärkungsmaßnahmen sowie Kommunikationsmaßnahmen zielen auf die **Empfänger:innen von Falschnachrichten**, so dass diese Falschnachrichten weniger Glauben schenken und sie weniger teilen.
2. Kommunikationsmaßnahmen setzen zusätzlich bei den **Absender:innen von Falschnachrichten** an, indem sie weniger Raum für Gerüchte und Spekulationen lassen und kursierende Falschnachrichten korrigieren. Meldungen an die Plattformbetreiber und Strafverfolgungsbehörden sowie das Löschen und Blockieren unterbinden aktiv die Kommunikation von Verfasser:innen von Falschnachrichten.
3. Zuletzt kann auch die Arbeit der **BOS-Mitarbeitenden** verbessert werden, indem diese geschult werden, indem interne Prozesse optimiert werden und indem BOS mit anderen Organisationen kooperieren. Unverzichtbar ist auch ein Social Media Monitoring, so dass die Mitarbeitenden wissen, welche Falschnachrichten wo kursieren.

Die folgende Abbildung zeigt auf, welche Maßnahmen sich an welche Zielgruppe(n) richten.

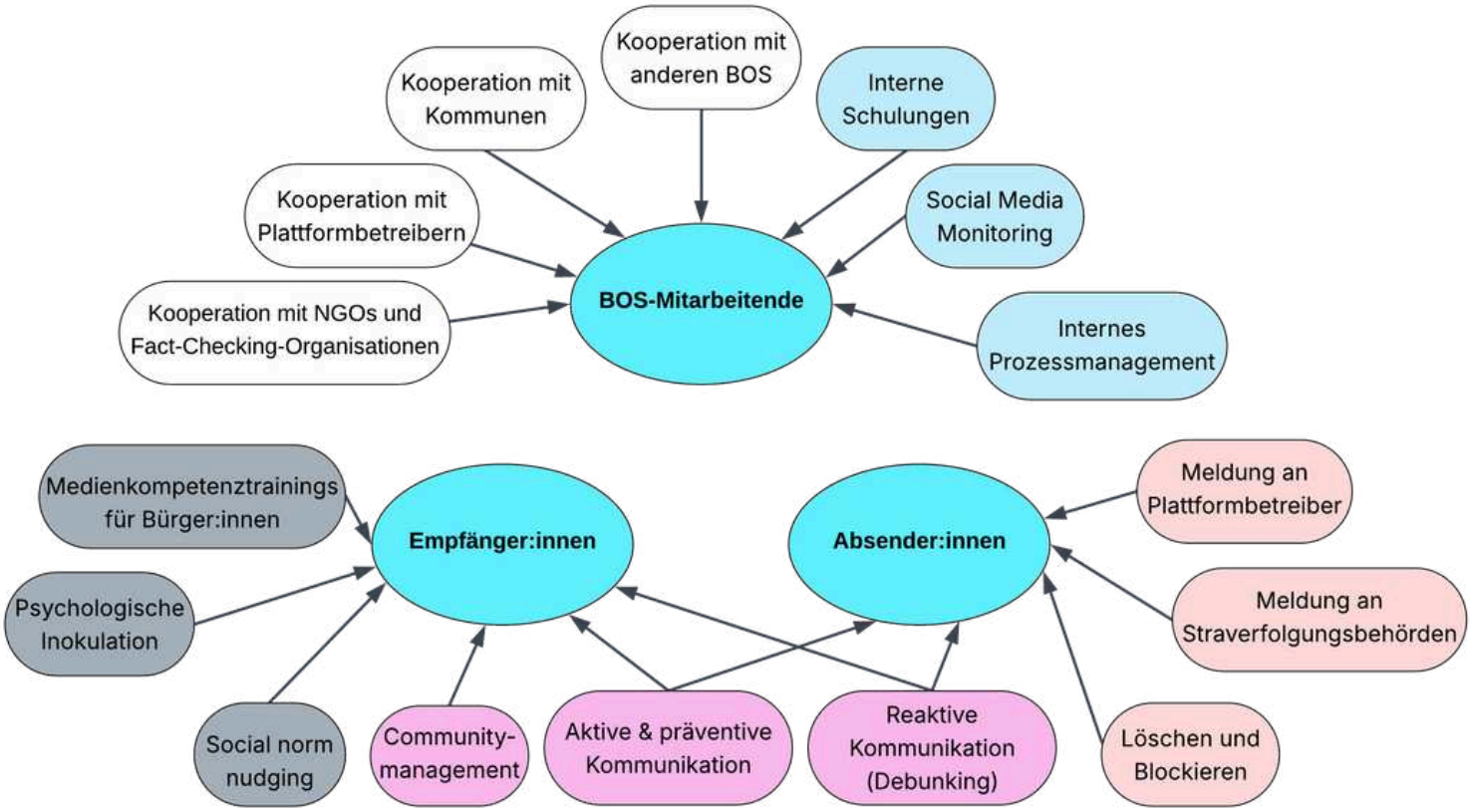


Abbildung 3: Zielgruppen möglicher Gegenmaßnahmen
Quelle: Eigene Darstellung

6.3 Zeitlicher Einsatz der Maßnahmen

Hilfreich kann auch sein, sich zu überlegen, wann verschiedene Maßnahmen zeitlich ansetzen. Helfen die Maßnahmen eher vorzubeugen, oder reagieren sie auf bereits kursierende Falschnachrichten? Je nachdem, in welchem zeitlichen Verlauf sich eine Lage befindet, können unterschiedliche Maßnahmen zum Einsatz kommen (vor, während oder nach der Lage) und entsprechend auch mit unterschiedlicher Intensität und unterschiedlichem Aufwand gerechtfertigt sein.

Nutzendenzentrierte Maßnahmen sind eher als **Vorbeugung** vor dem Kontakt mit Falschinformationen gedacht. Auch interne Vorbereitungen, wie Schulungen und der Aufbau eines guten Prozessmanagements, sind Aufgaben, die vor den Lagen passieren sollten. Communitymanagement ist ebenfalls eine langfristige und vorbeugende Aufgabe, die durchgängig erfolgt.

Social Media Monitoring ist zwar ebenfalls ein durchgängiger Prozess, weil sicherheitsrelevante Falschinformationen auch selbst Lagen hervorrufen können. Es wird aber in einer konkreten Krise besonders wichtig. Auch der Aufbau guter Kontakte und das Netzwerken mit Organisationen wie anderen BOS und Fact-Checking-Organisationen kann helfen, BOS vorbeugend zu stärken, sowie der **konkreten Krisenbewältigung** dienen.

Gerade zu Beginn von und während Krisen ist darüber hinaus eine vorbeugende und präventive Kommunikation wichtig, weil sie dazu beitragen kann, Falschinformationen vorzubeugen und die Folgen von Krisen abzumildern. Wenn Falschinformationen in einer Lage bereits kursieren, müssen BOS gegebenenfalls reaktive Maßnahmen einsetzen, insbesondere eine reaktive Krisenkommunikation (Debunking). Weitere Möglichkeiten sind das Melden von Falschinformationen an Plattformen und/oder Strafverfolgungsbehörden (diese Maßnahmen sind praktisch, ethisch und rechtlich jedoch problematisch, siehe Kapitel 11).

Die folgende Abbildung zeigt schematisch auf, wann verschiedene Maßnahmen ansetzen.

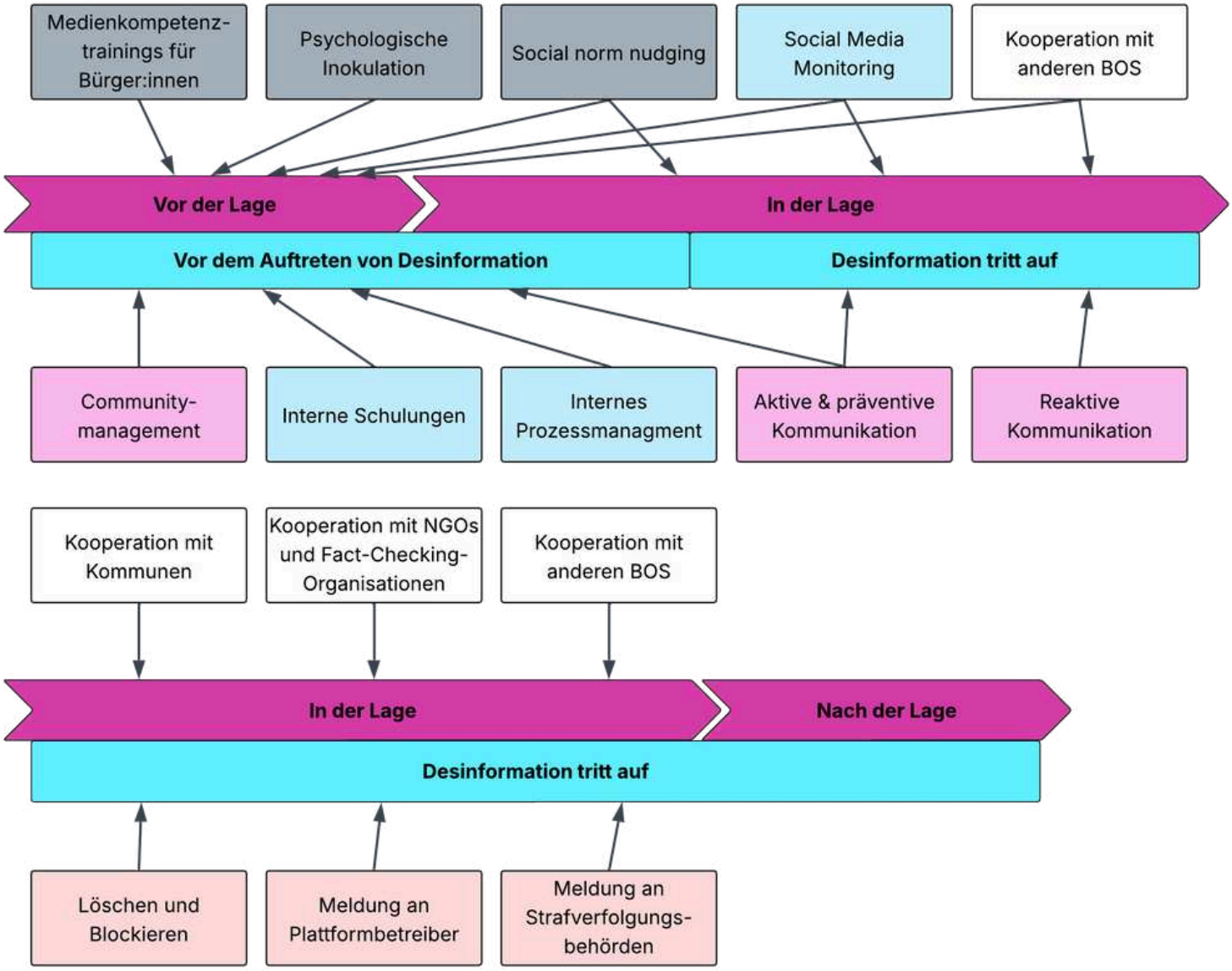


Abbildung 4: Zeitlicher Einsatz möglicher Gegenmaßnahmen
Quelle: Eigene Darstellung

7. Nutzendenzentrierte Maßnahmen

7.1 Förderung von Medienkompetenz

7.1.1 Grundlagen zur Förderung der Medienkompetenz

Die Verbesserung der Medienkompetenz der Bürger:innen gilt als **Schlüsselmaßnahme** zur Bekämpfung von Falschinformationen (Stroud 2019; Vese 2022). Die Bürger:innen sollen darin geschult werden, Desinformation und die Strategien böswilliger Akteure zu erkennen. Sie sollen beispielsweise lernen, Informationsquellen in den sozialen Medien zu überprüfen, Schlagzeilen und Inhalte kritisch miteinander und mit vertrauenswürdigen Seiten zu vergleichen, die Bilderrückwärtssuche zu nutzen und keine zweifelhaften Informationen weiterzugeben. Wenn Bürger:innen eine höhere Medienkompetenz haben, soll dies dazu führen, dass sie weniger falsche Informationen glauben und verbreiten.

Die wissenschaftliche Literatur sieht vor allem **Schulen, Medien und Institutionen der politischen Bildung** in der Verantwortung für diese Bildungs- und Aufklärungsarbeit (Mason et al. 2018; McDougall 2019). Interessanterweise nennt die Literatur BOS nicht als mögliche Akteure, die solche Trainings anbieten könnten oder sollten.

Es ist aber durchaus denkbar, dass **BOS solche Schulungen oder andere Maßnahmen (z.B. Online-Sensibilisierungskampagnen) zur Medienkompetenz anbieten** könnten bzw. sollten, soweit dies zu ihren Aufgaben der **Abwehr von Gefahren für die öffentliche Sicherheit und Ordnung** durch Falschinformation gezählt werden kann (siehe Kapitel 4.). So könnten BOS Präventionsvideos und andere Informationen zu Falschinformationen in den sozialen Medien veröffentlichen, oder entsprechende Schulungen für ihre Mitarbeitenden, aber auch für ehrenamtlich Engagierte oder eine breitere Öffentlichkeit zur Verfügung stellen. Allerdings fehlt es BOS häufig an den notwendigen Ressourcen, oder das Anbieten von Medienkompetenzschulungen liegt außerhalb ihres originären Aufgabenbereichs und ist hinsichtlich der Zielgruppe durch vorrangige Kompetenzen und erhöhte Anforderungen beschränkt (siehe Kapitel 7.3.).

Ein Beispiel für eine Online-Sensibilisierungskampagne einer deutschen Sicherheitsbehörde sind die Präventionsvideos des Projekts „Zivile Helden“ des Bundesprogramms Polizeiliche Kriminalprävention, das mit einem Präventionsvideo und einem begleitenden Quiz Zivilcourage im Umgang mit Online-Hass (und anderen Phänomenen) fördert. Allerdings geht es bei dieser Kampagne nicht direkt um Falschinformationen (siehe Beispiel “Zivile Helden”).

7.1.2 Ethische Überlegungen zur Förderung von Medienkompetenz

Die Schulung von Bürger:innen, Freiwilligen und Mitarbeitenden in Medienkompetenz und kritischen Fähigkeiten steht grundsätzlich im **Einklang mit demokratischen Werten**: Schließlich ist es ein wichtiges Ziel pluralistischer Demokratien, ihre Bürger:innen dabei zu unterstützen, informiert zu sein und kritisch zu denken, damit sie sich sinnvoll am politischen Prozess beteiligen können. Medienkompetenztrainings können Einzelne in die Lage versetzen, zwischen korrekten und irreführenden Informationen zu unterscheiden. Sie fördern daher zielführende und erfolgreiche demokratische Debatten als Grundlage des demokratischen Prozesses (siehe Kapitel 1.2). Sie können außerdem die **Sicherheit erhöhen**, wenn eine hohe Medienkompetenz den Bürger:innen hilft, bei Gefahren und Krisen Falschinformationen zu erkennen und weniger davon zu verbreiten. Grundsätzlich liegt es daher auch im Interesse von BOS, Medienkompetenztrainings zu unterstützen oder – sofern Ressourcen vorhanden sind – sogar selbst anzubieten.

BOS müssen dabei jedoch einige praktische, ethische und rechtliche Punkte (siehe Kapitel 7.3) beachten: Aus praktischer Sicht müssen Medienkompetenzmaßnahmen angesichts der Informationsflut online immer professionell aufbereitet und zudem wiederholt angeboten werden, um die gewünschte Wirkung zu erzielen. Das ist natürlich ressourcenintensiv (W03).

Darüber hinaus müssen die Medienkompetenzkurse selbst **ethischen und demokratischen Standards** genügen. So dürfen z.B. staatliche Quellen nicht generell oder ausschließlich als vertrauenswürdig und nicht-staatliche Quellen als nicht vertrauenswürdig eingestuft werden. Außerdem haben die BOS hier eine besondere Verantwortung, alternative Meinungen und staatskritische Medien nicht zu unterdrücken oder bestimmte Gruppen per se negativ darzustellen. Medienkompetenztrainings dürfen darüber hinaus nicht parteiisch sein, insbesondere wenn sie von staatlichen Stellen angeboten werden.

Wichtig ist es auch, **realistische Erwartungen an die Wirkung** von Medienkompetenztrainings zu haben. Sie können nicht dazu beitragen, politische Gräben zu überbrücken (boyd 2018a; boyd 2018b). Es ist also unwahrscheinlich, dass Bürger:innen, die beispielsweise klassischen Medien, wie Online-Ablegern von etablierten Zeitungen, misstrauen und Verschwörungsideologien anhängen, durch Medienkompetenztrainings erreicht werden können.

7.1.3 Rechtliche Überlegungen zur Förderung von Medienkompetenz

Viele Verantwortliche in Politik, Wissenschaft und Wirtschaft sehen mittlerweile die Notwendigkeit verstärkter Medienbildung. Alle kommen zum selben Ergebnis: Die Vermittlung und Förderung von Medienkompetenz ist eine dringliche **gesamtgesellschaftliche, aber doch zuvörderst staatliche Aufgabe**. Sie schließt alle Altersgruppen ein und muss insbesondere von den Schulen und den Einrichtungen der Erwachsenenbildung wahrgenommen werden. Die digitale Medienkompetenz soll die Nutzenden letztlich dazu befähigen, das Internet selbstbestimmt, kompetent und souverän zu nutzen. Dabei geht die Hauptverantwortung für deren Vermittlung und die entsprechenden Initiativen von staatlicher Seite aus (hierzu der Aktionsplan der Europäischen Union für digitale Bildung 2021-2027).[3] Es finden sich Ansätze zu einer solchen Medienbildung in den Förderungsansätzen des Bundesministeriums für Bildung, Wissenschaft und Forschung (BMBF 2022). Kritisch muss jedoch die **Förderung der (Digital-)Medienkompetenz bei Schüler:innen und Kindern durch BOS** betrachtet werden. Soweit es um die Bildung der Schüler:innen geht, kommt Art. 7 Abs. 1 GG zum Tragen: Demnach untersteht das gesamte Schulwesen der Aufsicht des Staates. Entsprechend liegt das Schulwesen aufgrund der Kompetenzverteilung im **Kompetenzbereich der Länder**. Hinsichtlich dieser Bildungsaspekte bei Kindern und Jugendlichen müssen Vertreter von entsprechenden Einrichtungen des Bundes deshalb darauf achten, nicht eigeninitativ die Kompetenz der Länder zu übergehen. Darüber hinaus haben die Eltern das Recht und die Pflicht, für ihre Kinder zu sorgen (Art. 6 Abs. 2 S. 1 GG). Dies umfasst die Aufgaben, sie zu beaufsichtigen, zu schützen und zu erziehen (GG-Badura, Art. 6 Rn. 24). Das gilt auch mit Blick auf die Nutzung digitaler Medien. Die **elterliche Sorge** ist notwendig, weil und solange das Kind noch nicht in der Lage ist, ein selbstbestimmtes Leben zu führen. Das gilt auch in Bezug auf die Mediennutzung: Je älter und reifer ein Kind ist, desto mehr ist seinem Bedürfnis nach selbstbestimmtem, verantwortungsvollem Handeln Rechnung zu tragen (§ 1626 Abs. 2 BGB).

Für das Kinder- und Jugendalter sind also vorrangig die Eltern für die Ausbildung der Medienkompetenz zuständig. Danach kommt dem Land eine Zuständigkeit zu, die er im Rahmen seiner Schulträgerschaft ausüben kann. **Erst im Erwachsenenalter sind die Rahmenbedingungen der Medienkompetenzbildung weniger streng**. Dann können BOS aktiv die betreffenden Nutzenden adressieren und ihnen unmittelbar Angebote zur Medienkompetenzbildung unterbreiten, ohne die **vorrangige Kompetenz von Eltern und dem Schulwesen** beachten zu müssen.

Insgesamt gilt: Auch bei der Förderung von Medienkompetenz müssen staatliche BOS die Grundsätze der Sachlichkeit, Neutralität und Richtigkeit beachten (siehe Kapitel 9.4).

[3] https://education.ec.europa.eu/de/focus-topics/digital-education/action-plan

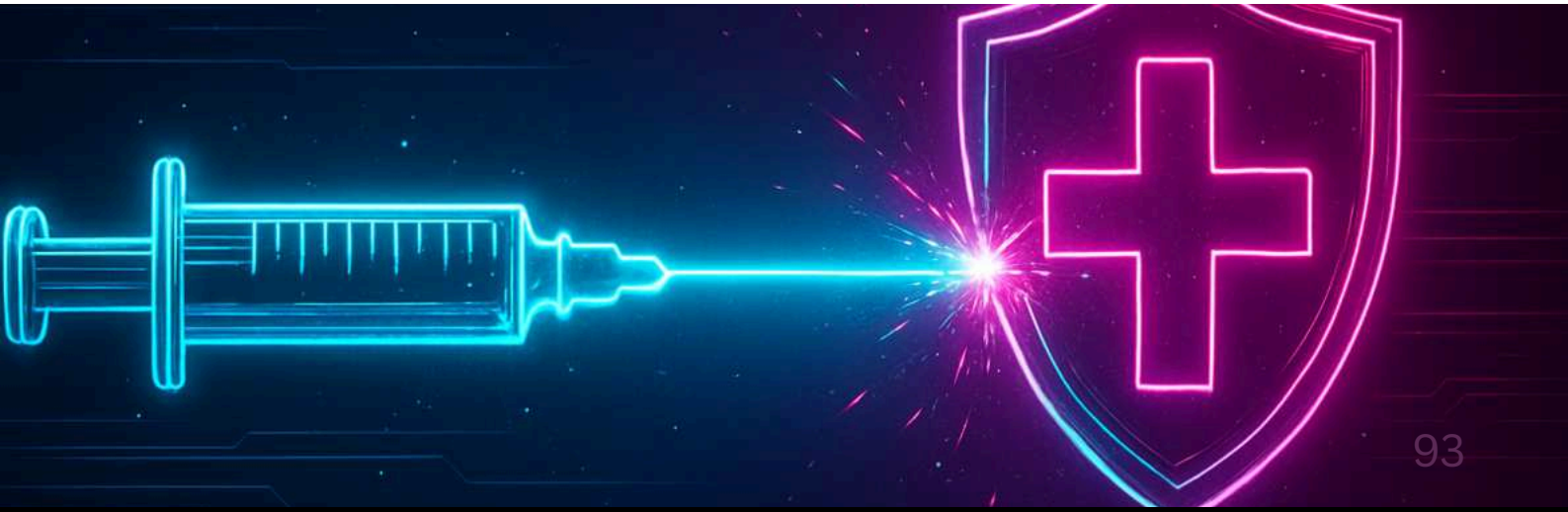
7.2 Inokulation

Medienkompetenztrainings sind die wohl naheliegendste Maßnahme, wenn es darum geht, die Widerstandsfähigkeit von Bürger:innen gegen Falschinformationen zu stärken. Die wissenschaftliche Literatur schlägt jedoch auch weniger bekannte Maßnahmen vor. Dazu gehört die so genannte “psychologische Inokulation“ (oder ”soziale Inokulation“), also eine Art **”Impfung“ gegen Falschinformationen** (Eccles und Dingler 2021; Eccles et al. 2021; Roozenbeek et al. 2022).

Diese Maßnahme zielt darauf ab, Menschen auf verschiedene Weisen mental auf Falschinformationen vorzubereiten und sie dadurch sozusagen “immun“ dagegen zu machen. Dabei ist die **Abgrenzung zu Medienkompetenztrainings nicht immer eindeutig**. Manche Beiträge sehen es z.B. auch als eine Form der Impfung, wenn vor Falschinformationen gewarnt wird, oder wenn Kenntnisse über typische Manipulationstechniken vermittelt werden (Roozenbeek und van der Linden 2019). Bildhafte, reale Beispiele von Prebunkingvideos sowie Fallstudien und passende interaktive Beispiele finden sich im Rahmen einer Initiative von Jigsaw und Google hier: https://prebunking.withgoogle.com/resources/.

Wir bezeichnen als psychologische Inokulation hier jedoch nur solche Maßnahmen, bei denen Menschen **zunächst vorgewarnt** werden, dass eine Konfrontation mit Falschinformationen droht. Dann werden ihnen **abgeschwächte Dosen an Falschinformationen “verabreicht“**, um sie “gegen stärkere, überzeugendere Botschaften“ zu impfen (Eccles et al. 2021; eigene Übersetzung). Daraufhin werden sie darüber **aufgeklärt**, dass diese Informationen falsch waren (und gegebenenfalls darüber, mit welchen Verschleierungstechniken und Manipulationsstrategien gearbeitet wurde).

Bisher scheint es so, dass BOS noch keine psychologische Inokulation gegen Falschinformationen betreiben.



7.2.1 Ethische Einschätzung

Maßnahmen, bei denen die BOS Bürger:innen falsche Informationen "verabreichen", um sie gegen Falschinformationen zu "impfen", sind aus mehreren Gründen problematisch. Zum einen würden sie voraussetzen, dass die BOS zu Schulungszwecken **selbst Falschinformationen verbreiten**. Das ist rechtlich und ethisch unzulässig, da staatliche Institutionen in besonderem Maße zu wahrheitsgemäßer, neutraler und objektiver Kommunikation verpflichtet sind (siehe Kapitel 9.4). Nicht bei allen Schulungsprogrammen oder Kampagnen können BOS sicherstellen, dass die Vorwarnung von allen Teilnehmenden verstanden wird und dass die klärenden Informationen unmittelbar danach gegeben (oder verstanden) werden und alle Nutzenden erreichen. BOS könnten somit unbeabsichtigt zur Verbreitung von Fehlinformationen beitragen. Da Korrekturen von Falschinformationen oft wenig Wirkung entfalten (siehe Kapitel 9.2), könnte dies schwerwiegende Folgen haben. Außerdem könnten einige Bürger:innen den Eindruck gewinnen, dass die BOS unwahre Tatsachen kommunizieren. Dies würde auch das **Vertrauen in sie als glaubwürdige Institution schwächen**.

Zweitens können Bürger:innen diese Impftechniken (trotz Vorwarnung) als **aggressiv und invasiv empfinden**, wenn sie mit Test- und Überraschungsmomenten arbeiten, insbesondere wenn zwischen der Vorwarnung und dem eigentlichen Angriff eine lange Zeitspanne liegt. Diese Maßnahme kann also weniger als selbstermächtigend denn als paternalistisch empfunden werden, da die Betroffenen von offizieller Seite mit ihren eigenen Fehlern konfrontiert werden, z.B. wenn sie darauf hingewiesen werden, dass sie die Nachrichten (möglicherweise) unvorsichtig gelesen haben und auf falsche Informationen hereingefallen sind. Hinzu kommt, dass die Wirkung dieser Maßnahmen möglicherweise **nur kurzfristig anhält** (Lu et al. 2023) und die dort präsentierten Falschinformationen das Vertrauen der Nutzenden in Medieninhalte weiter erschüttern können.

7.2.2 Keine Option?

Es ist aber nicht gänzlich ausgeschlossen, dass BOS die psychologische Inokulation nutzen könnten, um Bürger:innen gegen Falschinformationen zu stärken. Um den genannten ethischen Bedenken zumindest teilweise zu begegnen, dürften sie die Maßnahme jedoch nur bei Nutzenden durchführen, die **vorher über die Methode und ihre Ziele informiert wurden und ihr zugestimmt** haben. Zudem sollte der "Angriff" mit Falschinformationen nach der Vorwarnung schnell erfolgen (Eccles und Dingler 2021).

BOS sollten außerdem **unpolitische und fiktive Beispiele** verwenden (s. Beispiel "Inoculation Science"). Dadurch können sie verhindern, als parteiisch und politisch nicht neutral wahrgenommen zu werden. Zudem wirkt dies abwehrenden Haltungen der Bürger:innen entgegen. Nicht zuletzt verringert es das Risiko, dass die BOS selbst zu einer Quelle der Desinformation werden.

7.3 Nudging

Die Fachliteratur zum Thema Falschinformationen schlägt als mögliche Maßnahme zur Bekämpfung von Falschinformationen das so genannte Nudging (“Anschubsen“) vor (Andı und Akesson 2021; Pennycook und Rand 2022). Das bedeutet, dass **Menschen auf subtile Weise in bestimmte Richtungen gelenkt**, aber nicht zu einem bestimmten Verhalten gezwungen werden. Menschen könnten z.B. dazu angehalten werden, die Richtigkeit von Beiträgen in sozialen Medien zu überprüfen.

Meistens können vor allem die Betreiber von Social Media Plattformen Nudges einführen. Beispielsweise könnten sie Nutzenden, die Links teilen wollen, eine Nachricht einblenden, welche die Nutzenden fragt, ob sie die Quelle überprüft haben. BOS können solche Nudges nicht umsetzen.

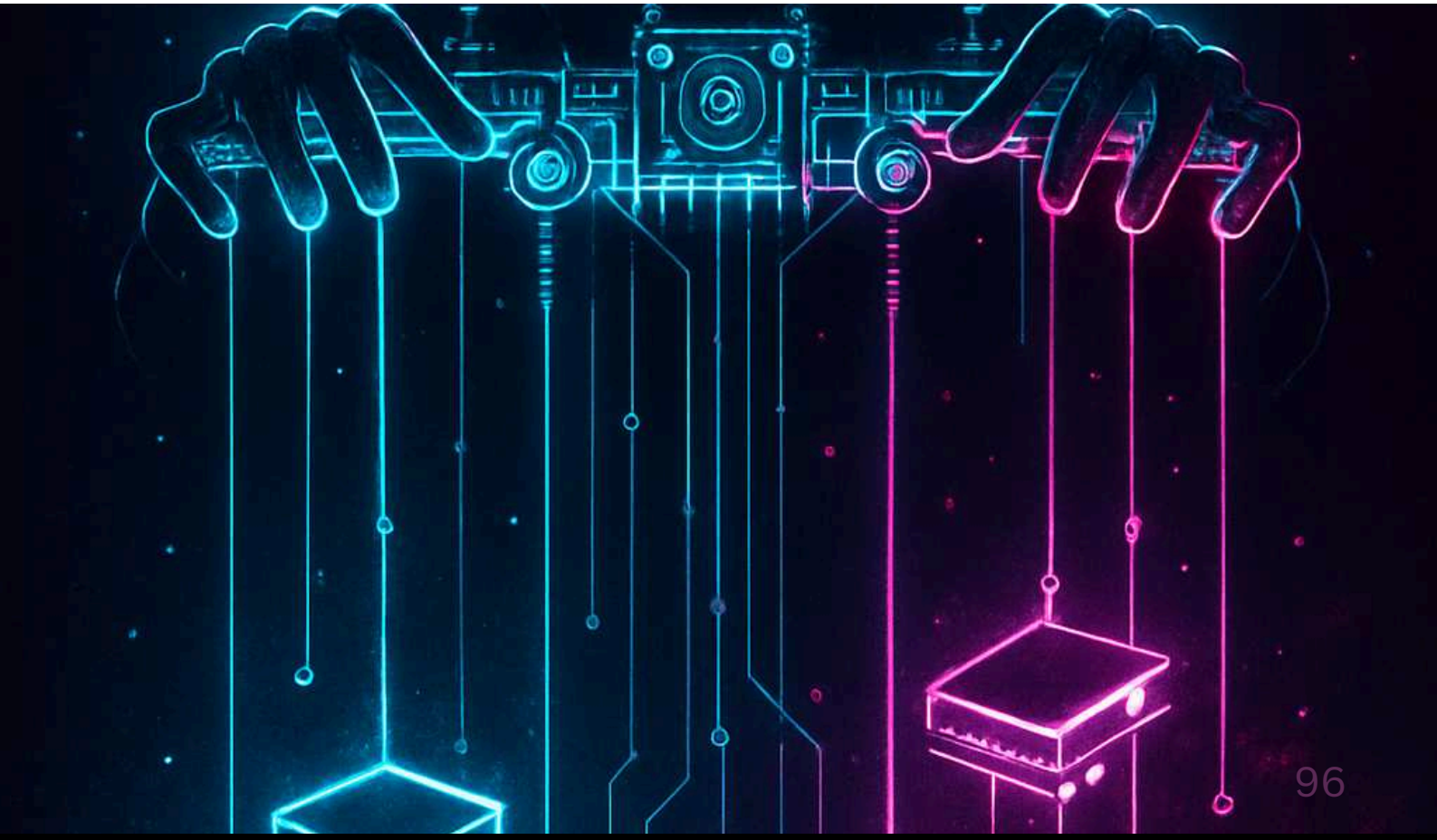
BOS könnten jedoch sogenannte **“Social Norm Nudges“** durchführen. Das heißt, sie könnten soziale Normen und Werte betonen. Dahinter steht die Erkenntnis, dass die meisten Menschen sich gerne an ihr soziales Umfeld und dessen Erwartungen anpassen. Sie richten sich gern nach den Verhaltensweisen, die andere vorleben, und nach den Werten, die von anderen erwartet werden. Social Norm Nudging bedeutet, dass diese Erwartungen und das angemessene Sozialverhalten so kommuniziert werden, dass die Empfänger:innen entsprechend handeln (Gimpel et al. 2021). BOS könnten beispielsweise darauf hinweisen, dass ein bestimmter Prozentsatz der Nutzenden sozialer Medien Beiträge meldet, wenn diese der Meinung sind, dass sie falsche Informationen enthalten. BOS könnten auch betonen, dass Nutzenden den Wahrheitsgehalt der von ihnen geposteten Links überprüfen sollten, um die Qualität ihrer Informationen für alle Follower:innen zu erhöhen. Damit würden sie die Werte, die in diesem Umfeld erwartet werden, aufzeigen. Beides könnte die Empfänger:innen dazu animieren, ihr eigenes Verhalten zu überdenken und gegebenenfalls an das Verhalten anderer bzw. die gängigen Werte anzupassen.

7.3.1 Ethische Einschätzung

Bisher scheinen BOS keine Social Norm Nudges einzusetzen, um Falschinformationen zu bekämpfen. Tatsächlich stellt sich für BOS die Frage, ob solche Hinweise nicht ihre **Neutralitätspflicht** verletzen. Hier muss jedoch eine Unterscheidung getroffen werden: Im Hinblick auf demokratische Werte spricht nichts dagegen, und es wäre sogar die Pflicht staatlicher Organisationen, Normen zu betonen, die sich ein demokratisches Gemeinwesen in Form seiner Gesetze und seiner demokratischen Verfassung gegeben hat. Als demokratische Institutionen sollten BOS nicht neutral sein, wenn es um Menschenrechte und demokratische Prinzipien geht.

Wenn BOS jedoch auch einen bestimmten Lebensstil durch Nudging fördern – z.B. eine bestimmte Art der Nutzung sozialer Medien – müssen sie sehr darauf achten, dass das Nudging **weder paternalistisch noch manipulativ** ist und dass es nicht bestimmte Gruppen und Meinungen im demokratischen Spektrum in ungerechtfertigter Weise **benachteiligt** (z.B. durch die Förderung einer rein konservativen oder neoliberalen Agenda, wie es Kritiker:innen befürchten; vgl. Pykett et al. 2011; Schnellenbach 2012).

In der Praxis ist Nudging außerdem **oft unwirksam** und kann sogar “nach hinten losgehen“ (Mols et al. 2015). So können entsprechende Nudges so ”umgedeutet“ werden, dass sie darauf hinweisen, dass ein (vermeintlich) großer Teil der Menschen ein sozial unerwünschtes Verhalten an den Tag legt. Damit würde dann das eigene Verhalten normalisiert. Ein Beispiel: Wenn BOS ihre Follower:innen dazu auffordern, eine bestimmte Falschinformation nicht weiterzugeben, die Empfänger:innen aber feststellen, dass diese Information dennoch weit verbreitet wird, wären entsprechende Hinweise auf soziale Normen unwirksam. Nudges können außerdem ins Leere laufen, wenn sich die Rezipient:innen nicht mit der jeweiligen Gruppe identifizieren, auf welche BOS verweisen.



Beispiel “Zivile Helden“

Ein Beispiel für eine Online-Präventionskampagne einer Sicherheitsbehörde ist das Projekt “Zivile Helden“ der Polizeilichen Kriminalprävention der Länder und des Bundes (ProPK). Das Projekt entstand im Rahmen eines interdisziplinären Forschungsprojektes (”Präventive digitale Sicherheitskommunikation – ein innovativer Ansatz für Kriminalprävention in sozialen Online-Medien“ (PräDiSiKo)), das 2016 bis 2019 vom Bundesministerium für Bildung und Forschung (BMBF) gefördert wurde.

“Zivile Helden“ ist eine **Internetseite mit interaktiven Videos** über Antisemitismus, Gewalt, Hass im Netz, Radikalisierung und Verschwörungsideologien. Die mit Deutsch-Rap untermalten Videos klären v.a. Jugendliche über die Themen und das richtige Verhalten in entsprechenden Situationen auf.

Keines der Videos behandelt speziell Falschinformationen. Die Themen Verschwörungsideologien, Radikalisierung im Netz und Hate Speech stehen jedoch im engen Zusammenhang mit dem Thema Desinformation.

Hier geht es zum Video zum Thema Hate Speech:
https://www.zivile-helden.de/hass-im-netz/

Hier geht es zum Video zum Thema Radikalisierung:
https://www.zivile- helden.de/radikalisierung/

Können Sie sich vorstellen, dass Ihre Behörde ähnliche Präventions- und Aufklärungsvideos produziert und bewirbt? Welche Vor- und Nachteile sehen Sie hier?

Beispiel “Swedish Psychological Defence Agency“

Die “Swedish Psychological Defence Agency” (schwedische Behörde für psychologische Verteidigung) ist eine **staatliche Behörde zur Bekämpfung von Desinformation und insbesondere von ausländischer Einflussnahme** z.B. aus China und Russland. Sie wurde 2022 gegründet.

Die Behörde **kooperiert mit Wissenschaftler:innen, dem Militär und den Medien und unterstützt regionale und nationale Behörden und Unternehmen** in Schweden dabei, Desinformation zu erkennen, zu analysieren und zu bekämpfen. Außerdem will sie die Resilienz (also die Widerstandsfähigkeit und Belastbarkeit) der **Bevölkerung** gegen Desinformation erhöhen.

Dazu betreibt die Behörde unter anderem eine Webseite mit dem Titel „Don’t be fooled!“ (Lass dich nicht täuschen!). Hier veröffentlicht sie sowohl auf Schwedisch als auch auf Englisch Informationen, um die breite Bevölkerung über Desinformation zu informieren.

Die “Swedish Psychological Defence Agency” hat außerdem vier kurze Videos produziert, um die Öffentlichkeit aufzuklären und widerstandsfähiger gegen Desinformation zu machen. In diesen sehenswerten Videos (schwedisch mit englischen Untertiteln) zeigen zwei schwedische Zauberkünstler, wie leicht Menschen zu manipulieren sind.

Hier können Sie sich die Videos ansehen:
https://www.youtube.com/@myndighetenforpsykologiskt7063/videos

Zur Aktivierung der englischen Untertitel klicken Sie rechts unten auf das Zahnrad.

Was halten Sie von dem Ansatz der Behörde, Videos mit Zauberkünstlern zu produzieren, um die Öffentlichkeit vor Desinformation zu warnen? Welche Vor- und Nachteile hat das? Können Sie sich so etwas auch im deutschen Kontext und vielleicht sogar für Ihre Behörde vorstellen?

Beispiel “Inoculation Science“

© University of Cambridge/University of Bristol/Jigsaw

Forschende an den englischen Universitäten Cambridge und Bristol haben in einem Experiment gemeinsam mit der Google Alphabet Tochtergesellschaft Jigsaw getestet, wie Inokulation in der Praxis funktionieren kann. Dazu haben sie **Videoclips kreiert, um Social Media Nutzende zunächst kurz mit einer typischen Manipulationsstrategie zu konfrontieren und sie dann darüber aufzuklären.** Die Videos wurden in mehreren Experimenten insgesamt fast 30.000 Teilnehmenden gezeigt, darunter auch Nutzende von YouTube (außerhalb eines eindeutig wissenschaftlichen Kontexts eines Experiments). Die Forschung konnte zeigen, dass bereits das einmalige Ansehen eines Filmclips das **Bewusstsein für Falschinformationen erhöht**.

Auf der Website des Projekts (https://inoculation.science/inoculation-videos/) können Sie sich die Videos auf Englisch ansehen.

Sollte es solche Videos auch auf Deutsch geben? Können Sie sich vorstellen, dass Ihre Behörde sich an einer solchen Kampagne beteiligt?

Die Lösungen zu den folgenden Quizfragen finden Sie auf den Seiten 175 f.

Frage 1

Was können Medienkompetenztrainings bewirken? (Mehrfachantworten möglich)

a) Sie können die Demokratie stärken, indem sie dazu beitragen, dass gezielte Desinformationen von ideologisch motivierten Akteuren, die die Demokratie schwächen und die Gesellschaft spalten wollen, weniger geglaubt und verbreitet werden.

b) Sie können die Sicherheit steigern, da Bürger:innen sicherheitsgefährdende Falschinformationen weniger glauben und auch weniger verbreiten.

c) Sie können Menschen, die Verschwörungsideologien glauben, „einfangen“ und ihnen verdeutlichen, welchen Quellen sie wirklich vertrauen können.

Frage 2

Wie müssen Medienkompetenztrainings gestaltet sein, um im Einklang mit demokratischen Werten zu stehen?

a) Sie sollten betonen, dass Bürger:innen insbesondere auf staatliche Quellen vertrauen sollten und nicht-staatlichen Quellen skeptischer gegenüberstehen sollten.

b) Sie sollten weltanschaulich möglichst neutral sein und Bürger:innen dazu befähigen, vertrauenswürdige von nicht-vertrauenswürdigen Quellen zu unterscheiden und Informationen kritisch zu hinterfragen.

c) Sie müssen professionell aufbereitet und wiederholt angeboten werden.

Frage 3

Welche Institutionen sollen insbesondere die Vermittlung und Förderung von Medienkompetenz wahrnehmen?

a) Schulen und Einrichtungen der Erwachsenenbildung

b) Private Organisationen

c) Nur staatliche Behörden

Frage 4

Wer ist vorrangig für die Ausbildung der Medienkompetenz im Kinder- und Jugendalter zuständig?

a) Schulen

b) Eltern

c) Der Staat

Frage 5

Was sollten BOS beachten, wenn sie Bürger:innen mit kleinen Dosen an Falschinformationen „impfen“ wollten (psychologische Inokulation)?

a) Bürger:innen müssen immer vorgewarnt werden und sollten mit der Maßnahme einverstanden sein.

b) Zwischen der Vorwarnung und der eigentlichen Konfrontation mit Falschinformationen sollte eine ausreichend lange Zeitspanne liegen, damit sich die Menschen mental vorbereiten können.

c) Es ist wichtig, reale Beispiele zu verwenden, um eine ausreichende Wirkung zu erzielen.

Frage 6

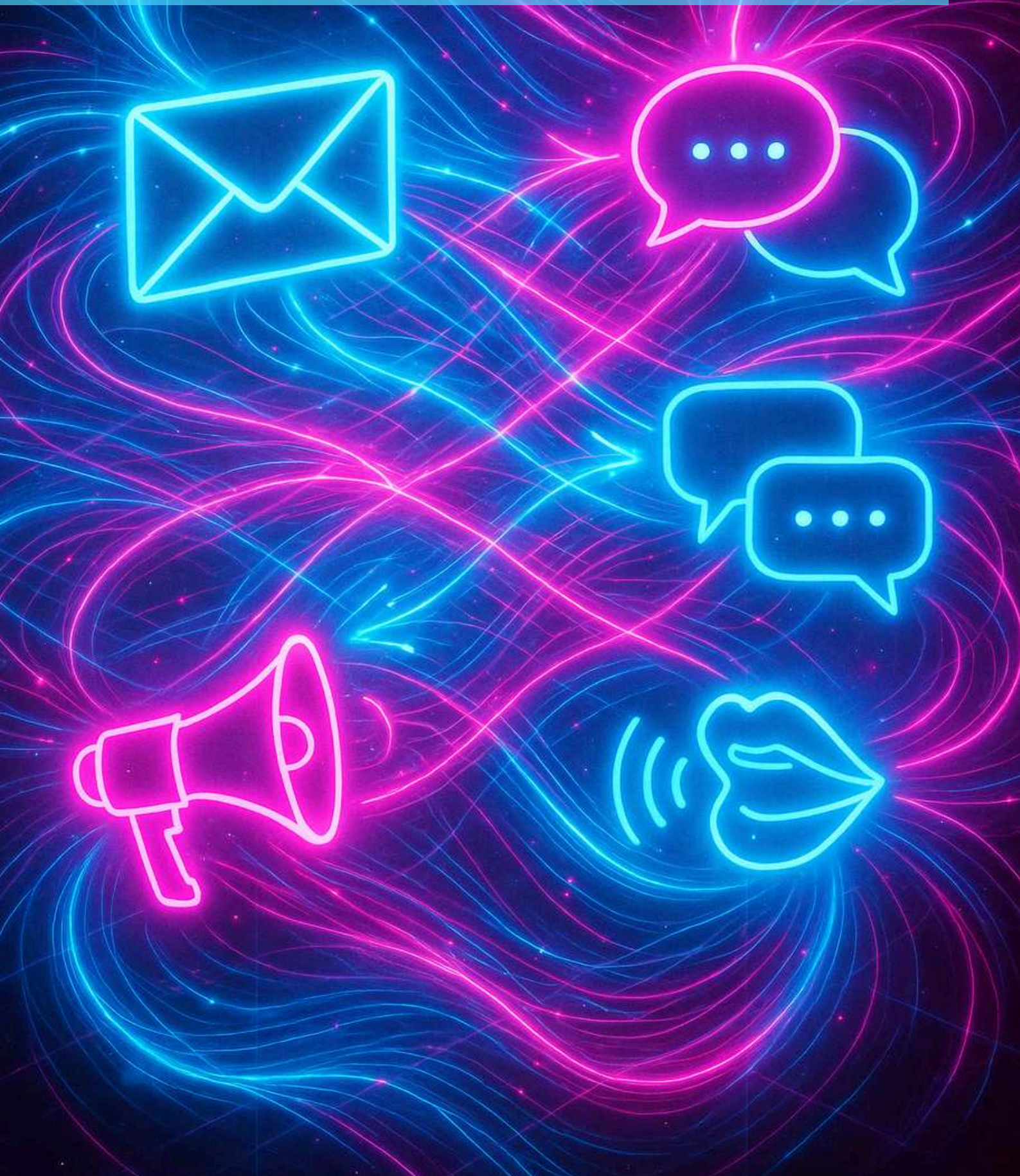
Social Norm Nudging, also die Betonung sozialer Normen und Werte…

a) … ist für BOS keine Option, da sie damit ihre Neutralitätspflichten verletzen.

b) … ist ressourcenintensiv und daher für BOS unrealistisch.

c) … kann „nach hinten losgehen“, wenn in der Realität viele Menschen ein sozial schädliches Verhalten vorleben, beispielsweise viele Menschen falsche Informationen teilen und verbreiten.

8. Interne Informationsbeschaffung, -priorisierung und -verifikation



8.1 Social Media Monitoring

Eine der Hauptaufgaben vieler Social Media-Abteilungen von BOS ist das Social Media Monitoring, d.h. die **Beobachtung und Analyse von Inhalten in den sozialen Medien**. BOS können nach Veröffentlichungen in den Sozialen Medien suchen, die ihre eigene Organisation und beispielsweise konkrete Einsätze betreffen, aber auch breiter nach sonstigen in Bezug auf ihre Arbeitsgebiete relevanten Beiträgen.

Mögliche Ziele des Social Media Monitorings sind es, ein **Stimmungsbild** über die eigene Organisation zu erhalten (I04), **kriminelles Verhalten** aufzudecken, **Sicherheitsgefahren** frühzeitig zu erkennen und in Krisen **Lageberichte** zu erstellen (I09), um die eigene Arbeit zu koordinieren und handlungsfähig zu bleiben (I10). Auch das Aufspüren von (sicherheitsrelevanten) **Falschinformationen** kann ein Ziel von Social Media Monitoring sein (I05).

Die sozialen Medien sind zu einem **unverzichtbaren Schauplatz der Meinungsäußerung, des gesellschaftlichen Lebens und der politischen Meinungs- und Willensbildung** geworden. Es wäre daher demokratietheoretisch nicht vertretbar, wenn BOS nicht über die dortigen Entwicklungen und Inhalte informiert wären. Dies würde zudem auch die BOS selbst gefährden, wenn sie von den Informationen der Sozialen Medien abgeschnitten wären und mögliche gefährliche Inhalte nicht kennen würden. Außerdem würde es BOS mit der Aufgabe der Gefahrenabwehr wie die Polizeibehörden unter Umständen sogar in der Erfüllung dieser Aufgabe beschränken. Doch welche praktischen Probleme und potenziellen Spannungsfelder zwischen verschiedenen Werten müssen BOS bei der Beobachtung der Sozialen Medien berücksichtigen?

Die Überwachung sozialer Medien erfordert einen großen Ressourceneinsatz (personell und finanziell). Gerade in Krisen und Katastrophen können einzelne BOS damit überfordert sein. Sie können dann gegebenenfalls **mit weiteren Organisationen zusammenarbeiten** (siehe Kapitel 4). In manchen Fällen kann das Social Media Monitoring einzelner Behörden insbesondere durch **VOST** (Virtual Operations Support Teams) unterstützt werden. Solche Teams gibt es auf Bundesebene (u.a. vom THW) sowie teils auf Landesebene. VOST-Teams bieten ein intensives Social Media Monitoring in Krisenfällen zur digitalen Lageerkennung und zur Verifizierung von Informationen an. Damit unterstützen sie anfordernde BOS (vgl. I09).

Unabhängig von einer möglichen Zusammenarbeit mit anderen Institutionen macht die Informationsflut im Internet ein gewisses Maß an Konzentration auf bestimmte Inhalte unerlässlich. BOS können ihr Social Media Monitoring daher **auf Posts über die eigene Organisation und ihre Einsätze beschränken** (vgl. I11). Themen, die die eigene Arbeit, aber nicht die Organisation selbst betreffen (also beispielsweise breitere Berichte über eine Flut, die nicht direkt mit konkreten Einsätzen der BOS in Verbindung stehen), würden von einem solchen Monitoring nur dann erfasst, wenn Mitglieder der Community sie entdecken und in den Social-Media-Gruppen der Organisation posten (siehe Kapitel 10) oder wenn Journalist:innen oder andere Personen von außerhalb die BOS auf relevante Themen hinweisen. Eine solche Fokussierung auf Beiträge über die eigene Institution und Arbeit ermöglicht einen pragmatischen Einsatz der eigenen Ressourcen, dient der Aufrechterhaltung der Legitimität und des Vertrauens in die eigene Institution und hilft zumindest, Inhalte zu finden, die mit höherer Wahrscheinlichkeit auch den eigenen Zuständigkeitsbereich betreffen. Darüber hinaus stehen die BOS in der Verantwortung, eine offene und möglichst unverfälschte Diskussion auf ihren eigenen Kanälen zu ermöglichen (W05). Angesichts der gesellschaftlichen und politischen Herausforderungen und Gefahren sicherheitsrelevanter Falschinformationen ist es jedoch fraglich, ob ein solch enger Fokus gerechtfertigt ist.

Ein **breiter angelegtes Social Media Monitoring** wirft jedoch eine Reihe ethischer und rechtlicher Fragen in Hinblick auf mögliche blinde Flecken und Diskriminierungstendenzen, Privatheit und Datenschutz und die Meinungsfreiheit auf, die in den folgenden Unterkapiteln (siehe zudem Kapitel 12.3 zum Social Media Monitoring) näher behandelt werden.

8.2 Verifizierung und Priorisierung

Unabhängig davon, wie breit BOS ihr Social Media Monitoring gestalten, müssen BOS prüfen, **ob aufgedeckte potenzielle Falschinformationen tatsächlich falsch** sind (Verifizierung). Zudem müssen sie überlegen, welche Falschinformationen in Bezug auf ihren Inhalt und/oder ihre Reichweite **schwerwiegender oder schädlicher** sind als andere beziehungsweise eine Reaktion erfordern (Priorisierung). Darüber hinaus müssen BOS sich für **mögliche Reaktionen entscheiden**, welche die öffentliche Meinungsbildung beeinflussen und zu teils erheblichen Nachteilen für einzelne Bürger:innen führen können. Hier treten Probleme der Abwägung zwischen zu bekämpfenden Falschinformationen und legitimer Meinungsäußerung sowie der Einschätzung der Sicherheitsgefahr einer Falschinformation in den Vordergrund. Was BOS bei diesen Fragen beachten sollten, wird in Kapitel 2 genauer behandelt.

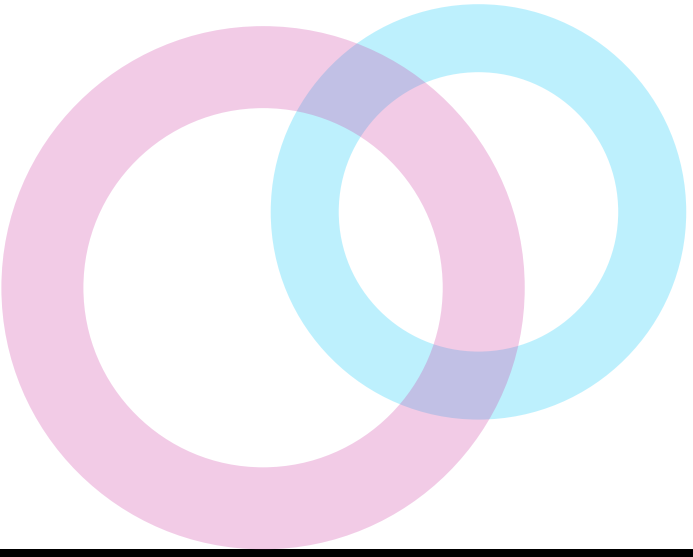
In diesem Zusammenhang ist als konkrete Maßnahme denkbar, dass BOS ihre organisationsspezifischen **Bewertungskriterien für Falschinformationen in Bezug auf Inhalt und Reichweite der Falschinformationen transparenter** gestalten. Diese Kriterien könnten dann auch wissenschaftlich und zivilgesellschaftlich überprüft und reflektiert werden. Darüber hinaus können BOS das **Mehr-Augen-Prinzip** anwenden, wenn sie eine Reaktion auf eine Falschinformation erwägen. Dies dient sowohl der Gerechtigkeit und Nichtdiskriminierung als auch dem Schutz der demokratischen Willensbildung.

8.3 Ethische Überlegungen zum Social Media Monitoring

Wenn BOS sich in ihrem Social Media Monitoring nicht nur auf die Nennung der eigenen Institution und ihre eigenen Einsätze konzentrieren, sondern ein breiter angelegtes Social Media Monitoring betreiben, wirft dies eine Reihe ethischer und rechtlicher Fragen auf.

Zunächst müssen BOS entscheiden, wie sie **nach welchen Arten von Informationen suchen**. Dabei können politisch und gesellschaftlich aufgeladene Suchbegriffe (und etwaige **“blinde Flecken“**) die (staatlichen) Reaktionen auf bestimmte gesellschaftliche Gruppen beeinflussen. Dies kann Ungerechtigkeit und Diskriminierung verstärken (Sievi und Pawelec 2025). Wenn BOS ihre Suchbegriffe z. B. auf linke Gewalt und Extremismus konzentrieren, können sie rechte Akteure oder ausländische Einflussnahme übersehen. BOS müssen daher reflektieren, wie sie ihre Suchen so gestalten können, dass sie Verzerrungen vermeiden, z. B. indem sie die jeweiligen Schlüsselwörter – und die verwendeten Sprachen – kritisch hinterfragen. Wenn deutsche BOS nur auf deutschsprachigen Kanälen nach falschen Informationen suchen, könnten sie beispielsweise Desinformation übersehen, die von böswilligen Akteuren in migrantischen Communities verbreitet wird.

Eine breitere Überwachung sozialer Medien ist auch im Hinblick auf die Privatsphäre und eine mögliche Überwachung der Bevölkerung problematisch, da BOS dabei zahlreiche Meinungsäußerungen der Bürger:innen überprüfen. Diese Meinungsäußerungen sind zwar öffentlich zugänglich. Bürger:innen hegen aber trotzdem gegebenenfalls eine gewisse **Privatheitserwartung** und gehen nicht davon aus, dass ihre Äußerungen systematisch behördlich erfasst und analysiert werden (Omand 2017; Bartlett et al. 2013). BOS müssen also auf "Verhältnismäßigkeit und Notwendigkeit" achten und "ein freies und offenes Internet" aufrechterhalten. Wenn sie dies nicht tun, schadet dies ihrem Ruf (Bartlett et al. 2013, eigene Übersetzung).



Wenn BOS Inhalte in den sozialen Medien analysieren, können darüber hinaus unmittelbar das **Recht auf Privatsphäre und der Datenschutz betroffen** sein, da die BOS beim Lesen und Prüfen der Inhalte in der Regel personenbezogene Daten verarbeiten. BOS müssen daher im "öffentlichen Interesse" handeln, um solche Informationen erheben und verarbeiten zu dürfen (Art. 6 Abs. 1 lit. e DSGVO; siehe Kapitel 5). Ein solches öffentliches Interesse ist in bestimmten Einsatzsituationen, z.B. bei Überschwemmungen und anderen Krisen, besonders eindeutig: Hier kann die Überwachung entsprechender Social-Media-Posts auf Falschinformationen unmittelbar die Sicherheit der Bevölkerung erhöhen. Doch auch die Funktionsfähigkeit staatlicher BOS kann unter Umständen zu einem solchen “öffentlichen Interesse“ gehören, soweit durch Falschinformationen die Wahrnehmung ihrer öffentlichen Aufgaben wie etwa die Gefahrenabwehr beeinträchtigt wird.

Doch selbst wenn ein öffentliches Interesse gegeben ist, müssen BOS stets prüfen, ob sie durch den Einsatz bestimmter technischer **Tools Datenschutzverletzungen umgehen oder mildern** können. BOS könnten also prüfen, ob sie Tools nutzen können, die Social-Media-Beiträge zur Erkennung von Trends aggregieren und anonymisieren oder, die es ermöglichen, Inhalte zu überprüfen, ohne personenbezogene Daten zu sammeln und zu verarbeiten.

Darüber hinaus kann die Überwachung sozialer Medien durch BOS größere **Bedenken in Bezug auf die demokratischen Freiheiten** aufwerfen: Allein das Gefühl, dass öffentliche Meinungsäußerungen von staatlichen Stellen mitgelesen werden, könnte zu einer verminderten politischen Beteiligung und verändertem Verhalten führen (Loh 2021). BOS könnten Bürger:innen mit allen Reaktionen auf Posts ein solches Gefühl vermitteln. Dies könnte dazu führen, dass Bürger:innen das Gefühl haben, ständig behördlich überwacht zu werden, und sich selbst zensieren – mit negativen Auswirkungen auf die Meinungsfreiheit (so genannte **“chilling effects“**; Warg 2018).

8.4 Rechtliche Überlegungen zum Social Media Monitoring

Wenn Daten aus sozialen Netzwerken erhoben werden, dann ist das nicht immer **verfassungsrechtlich bedenklich**. Werden aber Daten mit dem Zweck erhoben, sie zur Datenauswertung eines Social Media Monitorings zu verwenden, sieht das anders aus – auch, wenn in dem Rahmen Massendaten aggregiert werden. Erst recht trifft dies natürlich zu, wenn BOS **gezielt nach dem Verhalten einer Einzelperson** fahnden. In solchen Fällen werden **u.a. die Persönlichkeitsrechte** der betroffenen Personen empfindlich verletzt. Dadurch, dass sich eine Person in die (digitale) Öffentlichkeit begibt, verliert sie nicht automatisch das Recht, selbst darüber zu bestimmen, wie ihre Daten und sonstige Informationen verwendet und dargestellt werden. Es ist gerade grundrechtlich verbürgt, dass die betroffene Person das Recht hat, in dieser Form von ihrer **Freiheit zur Selbstdarstellung** Gebrauch zu machen. Stichworte sind hier besonders die **"informationelle Selbstbestimmung"** als Teil des **allgemeinen Persönlichkeitsrechts (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG)** und wieder die **Meinungsfreiheit (Art. 5 Abs. 1 S. 1 GG**; Venzke-Caprarese 2013: 779). Die Meinungsfreiheit ist vor allem aufgrund der realen Gefahr einer möglichen Selbstzensur schnell beeinträchtigt, wenn Bürger:innen den Eindruck bekommen sollten, unter ständiger **staatlicher Beobachtung** zu stehen.

Dass Daten und persönliche Informationen in der besonders weiten und allgegenwärtigen Öffentlichkeit in sozialen Netzwerken an einen weiten Kreis von Nutzenden getragen werden, macht sie also **nicht weniger schutzwürdig** (Desoi 2018: 176). Zugleich ist es aber auch widersprüchlich, sich auf die Privatheit von Informationen zu berufen, wenn diese hochgeladen und damit einem unbestimmten Personenkreis zur Verfügung gestellt werden. Immerhin wird mit einem solchen Vorgehen impliziert, dass diese Informationen nicht vollumfänglich vertraulich seien. Behörden, die öffentlich verfügbare Inhalte, welche für einen breiten Personenkreis zur Verfügung gestellt wurden, wahrnehmen und verwerten, **greifen somit nicht automatisch in die Grundrechte der betroffenen Person ein**. Der Spielraum zur Verwendung ist somit größer.

Dennoch bedarf es auch im frei zugänglichen, öffentlichen Raum einer **Rechtfertigung solcher Maßnahmen** (Venzke-Caprarese 2013: 777). Nicht immer ist etwa klar, ob die betreffenden Inhalte von dem/der anvisierten Nutzenden ins Netz gestellt wurden. Die/der Betroffene hat nicht zwingend alles, was der Öffentlichkeit zugänglich ist, selbst ins Internet gestellt. Vor allem aber wird dadurch, dass eine Person Inhalte ins Netz hochlädt, nicht automatisch impliziert, dass die Betroffenen mit jedweder Einsichtnahme – insbesondere durch staatliche Stellen – sowie jeglicher Form der Verwendung und Weiterverarbeitung einverstanden sind.

Eine erste Grenze staatlicher Informationserhebung und -auswertung (mittels Social Media Monitoring) liegt in der **Inanspruchnahme einer besonderen Vertraulichkeit durch die Nutzenden**. Nutzende haben diverse Möglichkeiten klarzustellen, dass im Rahmen dieser Art **"öffentlicher Privatheit"** (Sevignani 2017: 250) ihre Inhalte nur für die Wahrnehmung durch bestimmte Dritte vorgesehen sind oder nur in bestimmter Weise verwendet werden sollen. Nutzende sozialer Netzwerke können beispielsweise die Datenschutzvoreinstellung entsprechend konfigurieren oder Inhalte nur für einen bestimmten geschlossenen Benutzendenkreis veröffentlichen. Dies könnte bereits darin gesehen werden, dass das eigene Profil nicht öffentlich geschaltet wurde, sondern als ein privates, wie dies etwa bei Instagram möglich ist.

Nicht undenkbar ist es darüber hinaus, wenn BOS den Weg gehen, im Rahmen des Social Media Monitorings und der Informationsbeschaffung in den sozialen Medien **mit den Nutzenden anonym direkt zu kommunizieren**. Es ist in der rechtlichen Wertung angesichts der Anonymität im Netz zwar umstritten, inwiefern die Nutzenden darauf vertrauen dürfen, dass sie nicht mit einer staatlichen Stelle kommunizieren (BVerfGE 120, 274). Missbrauchen staatliche BOS aber diese Vertraulichkeit, greifen sie in das Grundrecht der Betroffenen ein und es bedarf für ihr Handeln einer bestimmten gesetzlichen Grundlage.

Eine weitere Grenze besteht dann, wenn der **Staat diverse Informationen und Daten gezielt zusammenträgt, speichert und auf eine Einzelperson bezogen auswertet**, ggf. unter Hinzuziehung weiterer Daten. Das derart konstruierte Gesamtbild aus Informationen, die sonst in keinem Zusammenhang miteinander stehen, verletzt die Betroffenen ebenfalls empfindlich in ihren grundrechtlich geschützten Positionen. Erstellt der Staat also Persönlichkeitsprofile und stellt das private und gesellschaftliche Leben unter Dauerbeobachtung, läuft er Gefahr, **durch den Eindruck der oder die tatsächlich bestehende Kontrolle die öffentliche und private Meinungsbildung zu stark zu beeinflussen**. Auch hier wäre die Folge wieder eine mögliche Selbstzensur, die bei den ethischen Überlegungen aufgegriffenen sog. **"chilling effects"** (GG-Grabenwarter, Art. 5 Abs. 1 Rn. 104). Ein möglichst offener und unbeeinflusster Austausch ist jedoch fundamental wichtig für ein **demokratisches Gemeinwesen**. BOS bedürften also wiederum einer **gesetzlichen Grundlage**, um dies tun zu dürfen. Es besteht bereits eine Auswahl an möglichen Gesetzesgrundlagen.

Wenn Sie dieses Training alleine absolvieren, nehmen Sie sich fünf bis zehn Minuten Zeit, um über die folgenden Fragen zu reflektieren.

Wenn Sie dieses Training in einer Gruppe absolvieren, reflektieren Sie zunächst 5 Minuten alleine über diese Fragen. Finden Sie sich dann in Zweiergruppen zusammen und diskutieren Sie Ihre Einschätzungen. Diskutieren Sie anschließend im Plenum.

1. Wenden Sie Social Media Monitoring in Ihrer Institution an? Wie erfolgt es? Wie verifizieren und priorisieren Sie (potenzielle) Falschinformationen?

2. Welche Vor- und Nachteile verschiedener Herangehensweisen beziehungsweise mögliche Gefahren sehen Sie hier?

3. Nach welchen Arten von Informationen sollte gesucht werden? Ist es gut/ legitim/ wünschenswert/ vernünftig, wenn sich BOS vor allem auf Nennungen ihrer eigenen Institution konzentrieren? Oder sollten sie breiter angelegt suchen? Warum? Warum nicht?

4. Zu welchem Grad darf Social Media-Kommunikation überwacht werden? Ist sie „öffentlich“? Welche Folgen könnte eine Überwachung haben?

5. Wie viel technische Unterstützung ist gut? Wo liegen hier die Gefahren? Was müssen Menschen (nicht mehr) machen?

Die Lösungen zu den folgenden Quizfragen finden Sie auf Seite 177.

Frage 1

Sind Social Media Posts öffentlich und dürfen BOS diese in der Folge frei analysieren?

a) Ja, schließlich kann sie jede/r lesen. Es ist daher auch ok, wenn BOS dies tun und auch analysieren, wer was gepostet hat.

b) Grundsätzlich schon. Allerdings erwarten viele Bürger:innen, dass gerade staatliche Behörden trotzdem nicht alles „mitlesen“ und analysieren. In anderen Worten: Sie erwarten ein gewisses Maß an Privatheit.

c) Nein. Da sie von Privatpersonen gepostet werden und sich an diese richten, sind sie privat.

Frage 2

Wie breit dürfen BOS die sozialen Medien nach Falschinformationen durchsuchen?

a) Überhaupt nicht, das wäre ja Überwachung!

b) Inhaltlich sehr breit - wenn es einen Anlass dazu gibt und der Datenschutz sowie die verfassungsrechtlichen Grenzen gewahrt bleiben. Schließlich dient das der Sicherheit!

c) Am besten BOS konzentrieren sich auf ihre eigene Organisation.

9. Präventive und reaktive (Krisen-) Kommunikation

9.1 Grundlagen

Eine gute Kommunikation und Öffentlichkeitsarbeit ist vermutlich das stärkste Mittel, das BOS gegen Falschinformationen in der Hand haben. Menschen glauben eher Falschinformationen, wenn zu einem Thema viel Unsicherheit vorherrscht und wenige gesicherte Informationen zur Verfügung stehen. BOS können daher mit der Veröffentlichung von passenden und richtigen Informationen in Krisensituationen das Informationsbedürfnis der Bevölkerung stillen und somit **Spekulationen und Gerüchten vorbeugen**. Dadurch nehmen sie Falschinformationen den Raum, um sich stärker ausbreiten zu können (I09).

Mit Kommunikation und Öffentlichkeitsarbeit meinen wir hier die Inhalte, die BOS insbesondere in den sozialen Medien und auf ihren Webseiten, aber auch über andere Kommunikationskanäle (z.B. Pressekonferenzen) veröffentlichen. Wir konzentrieren uns auf jene Veröffentlichungen, die dazu beitragen sollen, die Bevölkerung vor Schaden und Gefahren zu schützen.

Wir unterscheiden hierbei zwischen *präventiver* Kommunikation und *reaktiver* Kommunikation. Eine **präventive Kommunikation** bedeutet, dass BOS vor oder in der Lage von sich aus wichtige Informationen veröffentlichen, die zum Schutz, zur Information und Beruhigung der Menschen wichtig sind. Beispielsweise könnten das Informationen sein, wo BOS gerade im Einsatz sind, oder regelmäßige Updates, wie die Gefährdungslage vor Ort aussieht. Auch Antworten auf Fragen, die die Menschen besonders umtreiben, können dazu gehören. Diese präventive Kommunikation nimmt nicht direkt Bezug auf Falschinformationen, sondern veröffentlicht und verteilt gut geprüfte Informationen. Dadurch beugt sie gegebenenfalls der Entstehung von Gerüchten und Spekulationen sowie einer möglichen Verbreitung von Desinformation vor. Das Ziel einer solchen Kommunikation ist, die Informationshoheit zu erlangen oder zu behalten.

Unter einer **reaktiven Kommunikation** verstehen wir jene Nachrichten von BOS, mit denen sie auf bereits kursierende Falschnachrichten reagieren. Eine solche Reaktion kann ein direktes “Debunking“ sein, das heißt, die Behörden verkünden z.B. in einer Pressekonferenz oder auf ihren Social Media Kanälen, dass bestimmte Aussagen nachweislich falsch sind. Dabei können sie auch direkt auf Posts von Nutzenden mit Falschinformationen reagieren. BOS können aber auch indirekt auf Falschinformationen reagieren, die in den sozialen Medien kursieren, indem sie diese nicht direkt ansprechen, aber passgenaue Gegeninformationen veröffentlichen.

9.2 Grundsätzliche ethische Überlegungen zur (Krisen-)Kommunikation

Aus ethischer Sicht ist es geboten, dass BOS die Menschen in Krisen informieren. Nur mit guten und rechtzeitigen Informationen sind Menschen dazu in der Lage, sich selbst bestmöglich zu schützen und gegebenenfalls in Sicherheit zu bringen. Eine gute Krisenkommunikation trägt somit dazu bei, **Schaden zu minimieren und Gefahren zu reduzieren**.

Doch was ist eine gute Krisenkommunikation? Grundsätzlich gilt, dass die Kommunikation von Behörden **neutral** (Wegner et al. 2020) und ohne überschießende Wertungstendenz sein muss. Zudem müssen die veröffentlichten Informationen **sachlich und richtig** sein (zu rechtlichen Anforderungen siehe Kapitel 9.4; siehe auch Dunckel 2020).

BOS müssen sich hierbei jedoch vor Augen halten, dass sie **nie vollkommen neutral** sein können. Jede:r Kommunizierende hat bestimmte Perspektiven, Standpunkte und auch blinde Flecken, die in die eigenen Aussagen implizit und oft unbemerkt mit einfließen. Zudem ist jede Aussage auch in bestimmte Kontexte eingebunden, die ebenfalls nicht völlig neutral sind. In diesem Sinne ist unvermeidlich, dass BOS auch dazu beitragen, die Meinungsbildung zu formen. Ihr Ziel sollte jedoch sein, negative und verhaltenssteuernde Effekte zu minimieren und den Lesenden möglichst wenig in Bezug auf deren Lebensführung vorzuschreiben.

In einem Bereich müssen und sollten BOS jedoch nicht vollkommen neutral sein: Als demokratische Institutionen vertreten sie demokratische Werte und Prinzipien. Die Grundrechte und unsere pluralistische Demokratie zu verteidigen, widerspricht natürlich nicht dem Neutralitätsgebot.

Darüber hinaus sollte eine gute *Krisenkommunikation* von BOS von bestimmten Werten getragen sein und diese reflektieren. Gabel und Krüger (2020) betonten hier, dass eine gute und **ethisch reflektierte Krisenkommunikation** folgendermaßen sein sollte:

- **gerecht,**
- **verantwortungsvoll,**
- **transparent,**
- **wertschätzend,**
- **befähigend**
- **und zuverlässig.**

In Bezug auf sicherheitsrelevante Falschinformationen ist es für BOS und deren Reputation entscheidend, dass ihre Nachrichten **richtig** sind, das heißt so gut geprüft, dass die BOS von ihrer Wahrhaftigkeit ausgehen können. Zudem ist BOS als demokratischen Institutionen an der **Transparenz ihrer Kommunikation und Wertschätzung der Bürger:innen** gelegen, indem sie diese als mündig anerkennen und mit ihnen respektvoll kommunizieren. Damit von BOS geteilte Informationen zur Sicherheit beitragen können, müssen sie die Bürger:innen in Gefahrensituationen auch schnell oder zumindest **rechtzeitig sowie zuverlässig** erreichen. Die BOS müssen außerdem verantwortungsvoll entscheiden, welche Informationen sie weitergeben können, und ob es auch gewichtige Gründe gibt, die entgegenstehen (wie Datenschutz oder Persönlichkeitsrechte). Informationen sollten zudem für die Bürger:innen befähigend sein, d.h., dass auf ihrer Basis sinnvolle Entscheidungen in Gefahrensituationen getroffen werden können. Zuletzt wollen BOS ihre Informationen auch **gerecht** verteilen, so dass möglichst viele Menschen die Informationen erreichen.

Fallbeispiel Amoklauf im Münchener OEZ-Einkaufszentrum 2016

Am 22. Juli 2016 tötete ein 18-jähriger Schüler im Münchner Olympia-Einkaufszentrum (OEZ) neun Menschen, verletzte fünf weitere durch Schüsse und erschoss sich anschließend, als er von der Polizei gestellt wurde, selbst (siehe Beispiel in Kapitel 1). Das (rechtsextreme) Motiv war lange unklar. Während und direkt nach dem Amoklauf kursierten zahlreiche Falschinformationen in den sozialen Medien, aber auch in Messengerdiensten. Dazu gehörte das Gerücht, dass es mehr als einen Täter gebe. Infolgedessen kam es zur panikartigen Flucht von Menschen aus Orten, die eigentlich sicher waren. Dabei verletzten sich mindestens 32 Menschen. Darüber hinaus erschwerten zahlreiche Falschinformationen die Arbeit der Polizei, die immer wieder zu vermeintlichen Schießereien und Geiselnahmen gerufen wurde.

Auch für die Münchner Polizei selbst war es laut ihrem Pressesprecher da Gloria Martins dabei schwierig, schnell an gesicherte Informationen zu kommen: “Wann kriegen Sie als Polizei davon mit, wie bekommen Sie davon mit und wie belastbar sind diese Informationen?” (Welty 22.07.2017). Zudem herrschte insbesondere in den ersten Stunden des Amoklaufs Ressourcenmangel: “Der Pressesprecher Marcus da Gloria Martins selbst war zuhause, als ihn der erste Notruf erreichte. Die Batterien seines Handys waren leer, der Chef unerreichbar. Die Pressestelle arbeitete im Notdienstmodus – kein guter Start.“ (SieberAdvisors GmbH 2025). Gleichzeitig kursieren in den sozialen Medien bereits zahlreiche Augenzeug:innenberichte sowie ein Livestream eines Bürgerjournalisten (ebd.).

Nichtsdestotrotz war der Amoklauf auch gekennzeichnet von einer transparenten und umsichtigen Kommunikation durch die Münchner Polizei und insbesondere durch ihren Polizeisprecher, die in der Folge hoch gelobt und mehrfach ausgezeichnet wurde (Welty 22.07.2017). Die Münchner Polizei nutzte intensiv die sozialen Medien, um schnell und direkt zu informieren und auch Gerüchte richtigzustellen.

Da Gloria Martins beschreibt dies so: „Wir waren also näher, viel näher am aktuellen Kommunikationszeitgeschehen, sei es denn jetzt in der Nachrichtenwelt als auch informell über Bürger, als wir das je zuvor waren. Und das hat uns natürlich auch ein Stück weit in die Lage versetzt, immer mal wieder auch so ein Korrektiv hinauszusenden, wenn wir festgestellt haben, dass ein Gerücht besonders dominant war.“ (Welty 22.07.2017)

Dabei nutzte sie “die sozialen Medien in vorbildlicher Weise zur Aufklärung, zur Warnung, zum Dementieren von Gerüchten, zur Deeskalation in mehreren Sprachen.” (SieberAdvisors GmbH 2025) Zentral war aber auch ein ruhiger und besonnener Auftritt des Pressesprechers nach etwa drei Stunden: ”Authentisch und klar vermittelte er, was die Stadt in dieser Situation dringend benötigte: Ruhe! Er gab weiter, was es bis zu dem Zeitpunkt zu sagen gab. Er setzte in den Kontext, erklärte Zusammenhänge, machte in klarer und bildhafter Sprache deutlich, was man nach knapp drei Stunden wissen konnte – und was eben nicht. Nicht mehr und nicht weniger.” (Welty 22.07.2017)

Die Polizei München nutzte daher sowohl die sozialen Medien (in mehreren Sprachen) als auch klassischere Kommunikationskanäle, um zu informieren, zu beruhigen, zu deeskalieren, und Falschmeldungen richtigzustellen.

Fallbeispiel Dr. Lisa-Maria Kellermayr

2021 teilte die österreichische Ärztin Dr. Lisa-Maria Kellermayr, die sich für Covid-19-Impfungen einsetzte, ein Video auf Twitter (heute: X) und schrieb dazu: "Heute in Wels: Eine Demo der Verschwörungstheoretiker verlässt den Pfad unter den Augen von Behörden und blockiert sowohl den Haupteingang zum Klinikum als auch die Rettungsausfahrt des Roten Kreuzes."

Der Tweet war nicht grundsätzlich falsch, “auch wenn das Krankenhaus später klarstellt, dass die Rettung die Straße in die andere Richtung nützen konnte und der Zugang zum Krankenhaus möglich war. Doch die Polizei [Oberösterreich] antwortet ihr mit einem Tweet, in dem sie von "Falschmeldung" spricht.“ (Milborn und Punz 30.07.2022).

Daraufhin diskreditierten Impfgegner die Ärztin in einer Verleumdungskampagne und sprachen Morddrohungen aus. Dr. Kellermayr löschte ihren Tweet und bat die Polizei zunächst privat und dann öffentlich um die Löschung ihrer entsprechenden Antwort, u.a. mit den Worten: “Dieser Tweet ist Grundlage für eine Flut an Beschimpfungen, Verleumdungen, Drohungen und größte Anstrengungen von Anhängern der Szene, mir größtmöglichen Schaden zuzufügen. Er dient als Begründung, mich eine Lügnerin zu nennen, eine Hexe.“ (Milborn und Punz 30.07.2022).

Die Polizei reagierte nicht; der Tweet besteht bis heute. Dr. Kellermayr wurde daraufhin zur Zielscheibe von Impfgegner:innen, die sie teils persönlich bedrohten und belästigten. Daraufhin musste sie vorübergehend ihre Arztpraxis schließen. Bitten an die Polizei um Unterstützung wurden ignoriert. Im Juli 2022 beging die Ärztin Selbstmord.

Der Fall zeigt, welche gravierenden Folgen öffentliche Einschätzungen von BOS, dass bestimmte Posts falsch sind, auf die Betroffenen haben können.

9.3 Kernfragen für ethisch reflektierte Krisenkommunikation

Eine gute Krisenkommunikation von BOS sollte von bestimmten Werten getragen sein und diese reflektieren. Um das zu ermöglichen, können BOS sich mehrere Kernfragen stellen, um ihre (Krisen-)Kommunikation im Zusammenhang mit Falschnachrichten ethisch zu reflektieren.

1. Wer wird (nicht) erreicht?

Wer wird informiert, d.h. wen erreichen BOS tatsächlich über ihre Informationskanäle? Gerade, aber nicht nur Krisen sind die Kommunikationsressourcen von BOS (Geld, Zeit, Personal, Aufmerksamkeit) begrenzt. BOS müssen diese Ressourcen gerecht verteilen und dürfen dabei nicht diskriminieren.

Dazu gehört auch, dass BOS gegebenenfalls bestimmte **gesellschaftlich marginalisierte Gruppen unter besonderem Ressourcenaufwand gesondert ansprechen** müssen, damit möglichst viele Gruppen gleichberechtigten Zugang zu ihren Informationen haben. Das können Menschen mit einem geringen bis gar keinem Internetzugang bzw. Zugang zu den Informationsplattformen der BOS sein wie ältere Bürger:innen, Menschen mit geringem Einkommen und Bildungsgrad, mit körperlichen oder geistigen Behinderungen, oder auch Menschen, deren Muttersprache nicht Deutsch ist.

Es ist eine **Frage der Gerechtigkeit**, ob bestimmte Gruppen durch ihren Zugang zu den Kommunikationskanälen von BOS einen Informationsvorsprung haben, der für sie überlebenswichtig oder zumindest sicherheitsrelevant sein kann, und ob andere Gruppen benachteiligt werden, nicht zuletzt weil falsche Informationen nicht in den von ihnen bevorzugten Medien korrigiert werden. Gerade in Krisenzeiten werden bestehende gesellschaftliche Ungerechtigkeiten oft verschärft und verletzliche Gruppen sind oft weniger in der Lage, sich zu schützen (Sellnow und Seeger 2013). Dazu kann auch eine unfaire Kommunikationsstrategie beitragen.

BOS sollten daher analysieren, welche Zielgruppen sie auf den Plattformen, auf denen sie ihre Informationen veröffentlichen, (nicht) erreichen, welche Gruppen vor allem in Krisensituationen informiert werden, welche Medien vor allem zur Verbreitung von Falschinformationen genutzt werden und welche Gruppen BOS durch ihre bisherige Kommunikationspolitik benachteiligen. Dazu könnten BOS auch mit ihren Zielgruppen interagieren, um herauszufinden, wie sie diese (noch) besser informieren können (Veil et al. 2011) – in und außerhalb von Krisen.

2. So schnell oder so genau wie möglich?

Sollten BOS präventiv und reaktiv so schnell oder so genau wie möglich kommunizieren? Beides sind wichtige Werte für eine verlässliche Kommunikation, die jedoch **nicht immer in Einklang miteinander gebracht** werden können. Vor allem in Gefahrensituationen benötigen die Bürger:innen rechtzeitig Informationen, um sich vorzubereiten und Entscheidungen über ihr weiteres Vorgehen zu treffen. Es hilft auch, Unsicherheiten und Ängste abzubauen, wenn die Behörden schnell zu den Gefahren und Fakten Stellung nehmen und ihr Wissen weitergeben (Veil et al. 2011). Schnelligkeit ist vor allem dann wichtig, wenn Falschinformationen bereits im Umlauf sind, denn so kann ihre Verbreitung eingedämmt werden.

Gleichzeitig ist es für BOS zentral, wahrheitsgemäß zu kommunizieren, um als glaubwürdige und verlässliche Quelle gelten, durch zuverlässige Kommunikation langfristig die Sicherheit zu erhöhen, die Autonomie der Bürger:innen zu fördern und gefährliche Situationen nicht selbst durch falsche Aussagen verschärfen (vgl. Sievi/Pawelec 2025). Um Beiträge vor einer Veröffentlichung eingehend zu verifizieren, braucht es jedoch Zeit, denn auch BOS fehlen in gefährlichen und unübersichtlichen Situationen oft zuverlässige und ausreichende Informationen. Auch sie müssen zunächst die Situation analysieren und die verfügbaren Informationen überprüfen, damit sie nicht versehentlich zur Quelle von Falschinformationen werden. Die Tatsache, dass BOS oftmals Zugang zu exklusivem Wissen haben (beispielsweise, da sie selbst in einer Lage tätig sind oder entsprechende Personalressourcen aufwenden), ist ein großer Vorteil, kann aber auch zum Problem werden, wenn sie ungewollt falsche Informationen verbreiten, die von vielen zunächst für wahr gehalten werden (Wegner et al. 2020). Gerade wegen ihres exklusiven Wissens, ihrer Verpflichtung zur Wahrhaftigkeit und ihres Rufs als besonders vertrauenswürdige Akteure haben BOS eine besondere Verantwortung, wahrheitsgemäß zu kommunizieren, auch wenn dies bedeutet, dass sie vielleicht langsamer informieren als andere Akteure.

Doch in Krisensituationen fehlt diese benötigte Zeit oft. Wie sollen BOS mit diesem Widerspruch umgehen? In Krisen, in denen die Gefahren einer langsamen Kommunikation so groß werden, dass die Wahrhaftigkeit sie nicht mehr rechtfertigen kann, empfehlen Gabel und Krüger (2020): "Erstens sollte **Transparenz über den Status der Informationen** herrschen. Unsichere Informationen gilt es also als solche zu benennen. Zweitens sollte die Warnung **befähigend** wirken. Sie sollte also Informationen über angemessene Reaktionen enthalten. Ergänzend dazu ist die **Entwarnung** bei falschen Informationen oder der Überwindung der Gefahr essenziell (Gabel und Krüger 2020). BOS sollten also in solchen **dringenden Fällen auch unsichere Informationen** kommunizieren, dabei aber auch die Rahmenbedingungen ihrer Kommunikation offenlegen und ehrlich kommunizieren. Dabei nehmen sie mögliche Reputationsschäden in Kauf, um die Sicherheit und Autonomie der Bürger:innen zu erhöhen. Gleichzeitig können BOS durch Transparenz gegenüber der Öffentlichkeit diesen Schaden auch minimieren, Vertrauen wieder aufbauen oder erhalten und die Abwanderung zu anderen Quellen, die schnellere Antworten versprechen, verringern (Veil et al. 2011).

3. Was muss geheim bleiben?

In einem demokratischen Staat ist die Transparenz des staatlichen Handelns und des gesellschaftlichen Geschehens ein notwendiger Wert. Sie ist entscheidend, damit Bürger:innen informierte und selbstbestimmte Entscheidungen treffen, Kritik üben und Vertrauen in die Behörden gewinnen können. Nichtsdestotrotz **können und dürfen BOS nicht immer alles kommunizieren**, was nötig wäre, um die Informationsbedürfnisse der Bevölkerung zu erfüllen und etwaige Falschinformationen zu zerstreuen. Manchmal müssen sie aus verschiedenen Gründen bestimmte Informationen geheimhalten: Dazu gehören **taktische Gründe**, wie die Notwendigkeit, es ermittelnden Kolleg:innen und der Staatsanwaltschaft vor Ort zu ermöglichen, ihre Arbeit zu erledigen (und damit den Rechtsstaat und die Sicherheit zu stärken; vgl. I01, I02). BOS können auch aus **Datenschutzgründen** rechtlich zur Zurückhaltung von Informationen verpflichtet sein (siehe Kapitel 5). Bei Todesfällen in Folge von Unfällen oder Katastrophen müssen BOS außerdem sicherstellen, dass sie zuerst die Angehörigen informieren und die **Persönlichkeitsrechte** der Betroffenen respektieren.

Informationen geheim halten zu müssen, die nötig wären, um Falschinformationen richtigzustellen, ist für die betroffenen Mitarbeitenden mitunter unangenehm. Es entsteht eine Dilemma-Situation, denn die Zurückhaltung untergräbt die Transparenz staatlichen Handelns. Darüber hinaus kann Misstrauen in der Bevölkerung entstehen, wenn sie das Gefühl bekommt, BOS hielten bestimmte Informationen zurück (Sellnow und Seger 2013). Das kann wiederum bestehende Krisen verschärfen.

Wie sollten BOS also vorgehen? Zuallererst müssen sie **rechtliche Vorgaben** erfüllen. Darüber hinaus müssen sie in Dilemma-Situationen abwägen, ob es **legitime Gründe für die Zurückhaltung bestimmter Informationen gibt, die stärker wiegen als eine mögliche gesteigerte Autonomie** der Bürger:innen und Erhöhung der Sicherheit, die durch die Informationen erfolgen könnte. Hierbei sollten BOS auch berücksichtigen, ob die Bürger:innen durch die größere Transparenz tatsächlich einen Mehrwert an Informationen erfahren, der ihnen in ihrer Situation hilft, sie stärkt und die Sicherheit erhöht.

4. Können Betroffene Widerspruch einlegen?

Die Einstufung eines Beitrags als Falschinformation durch BOS (und insbesondere durch staatliche Behörden) kann gravierende Folgen für die Betroffenen haben – unabhängig davon, ob sie sachlich richtig ist oder nicht (siehe Fallbeispiel Dr. Lisa-Maria Kellermayr Kapitel 9). BOS tragen daher eine besondere Verantwortung dafür, dass ihre Handlungen **rechenschaftspflichtig** bleiben und angefochten werden können. Daher wäre es ethisch wünschenswert, dass die Verfassenden von vermeintlich falschen Beiträgen gegen diese Einstufung durch BOS **formell Widerspruch oder Beschwerde** einlegen können. Im Idealfall sollte dann eine unabhängige Stellen diese Einstufung überprüfen. Darüber hinaus sollten BOS ihre eigenen Fehler transparent machen, wenn sie ihre Bewertung von Informationen ändern oder wenn sie selbst falsche Informationen veröffentlicht haben (vgl. Sievi/Pawelec 2025).

5. Wie sollten BOS auf Kritik an der eigenen Organisation reagieren?

Schließlich müssen BOS-Mitarbeitende Werturteile fällen, wenn es darum geht, auf als falsch empfundene Kritik an der eigenen Organisation oder gar auf ernen sogenannten “Shitstorm“ zu reagieren, also auf einen ”Sturm der Entrüstung in einem Kommunikationsmedium des Internets, der zum Teil mit beleidigenden Äußerungen einhergeht“ (Duden 2025). BOS sehen sich relativ häufig mit solcher Kritik konfrontiert, die oft als falsch empfunden wird (Pawelec und Sievi 2023).

Das Dilemma für BOS besteht darin, dass falsche Behauptungen das **Vertrauen in sie und ihre Legitimität als demokratische und rechtsstaatliche Institutionen** untergraben. Andererseits ist es in einer Demokratie **unabdingbar, dass Bürger:innen (und Medien und zivilgesellschaftliche Organisationen) legitime und korrekte Kritik** an der Regierung und den Behörden äußern können, um so ihre demokratische Kontrolle auszuüben.

Die Behörden müssen daher in der Lage sein, Kritik bis zu einem gewissen Grad zu ertragen. Dabei müssen sie berücksichtigen, dass Kritik, selbst wenn es sich um falsche Informationen handelt, Elemente der Meinung enthalten und zum Ausdruck bringen kann (siehe Kapitel 3).

Wenn BOS Kritik an der eigenen Institution vorschnell und undifferenziert als “falsch“ oder gar als Desinformation (also als bewusst falsch) einstufen, besteht die Gefahr, dass kritische Äußerungen unangemessen schnelle, heftige und damit unverhältnismäßige Reaktionen hervorrufen. Dies würde die Meinungs- und Informationsfreiheit beeinträchtigen (d. h. die bürgerlichen Freiheiten unverhältnismäßig einschränken) und die demokratische Kontrolle der Behörden untergraben. Bevor BOS auf Kritik an ihnen reagieren, sollten sie daher sorgfältig **prüfen, ob diese Kritik gerechtfertigt ist, ob es sich um eine legitime Meinungsäußerung** handelt und ob die **gewählte Reaktion verhältnismäßig** ist (vgl. Sievi/Pawelec 2025).

Weiterführende Materialien zu einer ethisch reflektierten Krisenkommunikation

Leitfaden für eine ethisch reflektierte Krisenkommunikation

Gabel, F. und Krüger, M. (2020), Leitfaden für eine ethisch reflektierte Krisenkommunikation: eine Analyse wertbezogener Spannungsfelder in der Krisenkommunikation, Internationales Zentrum für Ethik in den Wissenschaften (IZEW), Universität Tübingen, abrufbar unter: https://uni-tuebingen.de/de/81680 (zuletzt geprüft am 07.02.2025).

Der Leitfaden entstand im Rahmen des Forschungsprojekts KOPHIS (Kontexte von Pflege- und Hilfsbedürftigen stärken – Verzahnung von BOS, Pflegeinfrastruktur und aktiven zivilgesellschaftlichen Netzwerken), das 2016-2019 vom Bundesministerium für Bildung und Forschung gefördert wurde. Er versteht sich als Schulungs- und Informationsmaterial, um Krisenkommunikationspraktiken ethisch zu hinterfragen und zu reflektieren.

9.4 Rechtliche Grundlagen staatlichen Informationshandelns

Staatliche Öffentlichkeitsarbeit im Sinne der Kommunikation mit der Bevölkerung hat die Aufgabe, die **Bürger:innen im demokratischen Sinne möglichst fundiert entscheidungsfähig** zu machen. Sie ist deshalb nicht nur darauf gerichtet, den Bürger:innen die staatliche Politik, Maßnahmen, Vorhaben sowie zukünftig zu lösende Fragen darzulegen und zu erläutern, sondern auch solche Informationen zu verbreiten, die die **Bürger:innen für ihre persönliche Meinungsbildung** benötigen. Auf Grundlage dieser Informationen können Bürger:innen an der **politischen Willensbildung im demokratischen Prozess teilhaben** (Duda et al. 2024: 381). Schließlich geht unser Grundgesetz von einer starken **Selbstverantwortung** seiner Bürger:innen aus und traut ihnen explizit die **eigenverantwortliche Mitwirkung** am politischen Geschehen zu.

Das Recht der staatlichen Öffentlichkeitsarbeit ist durch einzelne Gesetze, Rechtsprechung und die rechtswissenschaftliche Literatur geprägt. Eine Grundbedingung für die Zulässigkeit der Öffentlichkeitsarbeit ist, dass sich diese **ausschließlich im Rahmen des zugewiesenen Aufgaben- und Zuständigkeitsbereichs** der jeweiligen staatlichen Stelle bewegt. Zudem muss die Information die **Gebote der Richtigkeit, Sachlichkeit und Verhältnismäßigkeit** (dazu unten mehr) wahren (BVerfGE 105, 279, 252; 113, 63; Eggers 2020: 70). Wenn der Staat Informationen veröffentlicht, hat dies außerdem den Vorteil, dass seine potentiellen Adressat:innen die Informationen nicht mehr selbst suchen müssen. Es kommt deshalb ein gewisser **Service- und Einsparungsgedanke** zum Tragen, wenn der Staat die Informationen ins Internet stellt, anstatt diese zu drucken und zu verteilen. Zusätzlich erfüllt der Staat dabei seine **Pflicht der Neutralität und Gleichbehandlung**, indem er alle potentiellen Adressat:innen auf demselben Wege erreicht (Gusy 2014: 85 f.).

Interessanterweise ist bislang die **Unterlassung von Publikumsinformation** (d. h. Aufklärung, Beratung, Verhaltensempfehlung, Warnung) noch in keinem Einzelfall für verfassungs- oder gesetzeswidrig befunden worden (Gusy 2014: 86 f.). Grundsätzlich können staatliche BOS damit **frei sowohl hinsichtlich des "Ob", als auch des "Wie" der Öffentlichkeitsarbeit** entscheiden. Die Diskussion dreht sich vielmehr um ein Zuviel an Kommunikation bzw. die Methoden und Ausgestaltung derselben als um unterbliebene Warnungen. Kommunikation und Information sollen nämlich **möglichst unbeschränkt, unbeeinflusst und unverfälscht** sein. Das gilt nicht nur für privates, sondern auch für staatliches Informationshandeln. Problematisch ist daher die Gefahr einer möglichen **Verhaltenssteuerung** durch Information. In solchen Fällen kommt ein Eingriff in die Grundrechte der Bevölkerung - wie etwa die Meinungsfreiheit - in Betracht. Es bedarf also einer **ausdrücklichen Ermächtigungsgrundlage** im Sinne einer gesetzlichen Befugnis zum Handeln, die eine solche Maßnahme vorsieht. Bei Polizei- und Ordnungsbehörden kommt im Falle fehlender Grundrechtsbeeinträchtigung zudem eine **Aufgabenzuweisung** in Betracht, indem gesetzlich ihre Zuständigkeit für bestimmte Sachverhalte staatlichen Informationshandelns vorgegeben wird (BVerwG MMR 2015, 479, 482; Schoch 2011, 196).

Unabhängig davon, ob die staatliche Behörde einer Ermächtigungsgrundlage bedarf oder nicht, müssen die von ihr geteilten (Gegen-)Informationen sachlich, verhältnismäßig und **richtig** sein. Letzteres ist eine besondere Herausforderung für BOS – insbesondere in Krisenlagen, in denen es schwer bis nicht oder zumindest nicht rechtzeitig möglich ist, herauszufinden, welche Informationen wahr und welche falsch sind. Sie müssen deshalb in verhältnismäßiger und zumutbarer Weise recherchieren, ob die von ihnen verbreiteten Informationen wahr sind (BVerfGE 105, 252, 272). Bei unklarer Sachlage kommt dem Staat nämlich eine Aufklärungspflicht zu. Dies kostet wiederum Zeit, was im Kampf gegen Falschinformationen besonders im Netz ein kritischer Aspekt ist. Da die Abwehr dringender Gefahren häufig schnelles Handeln unter den Bedingungen unvollständiger Sachverhaltskenntnis erfordert, müssen staatliche BOS nach zeitlich möglicher Sachverhaltsaufklärung übrig gebliebene Unsicherheiten kenntlich machen.

Das Gebot der **Sachlichkeit** bedeutet darüber hinaus, dass Wertungen staatlicherseits vermieden werden sollen (BVerfGE 57, 1, 8). Dies bezieht sich nicht nur auf die inhaltliche Wertungsfreiheit, sondern auch auf die Darstellung von Fakten. Die verbreiteten Informationen müssen darüber hinaus auch **verhältnismäßig** sein (BVerfGE 105, 279, 309). Sind mit ihrer Veröffentlichung also Nachteile für Betroffene verbunden, müssen sie sich auf das zur Informationsgewährung Erforderliche beschränken.

Abschließend müssen staatliche Behörden bei ihrer Öffentlichkeitsarbeit das **Neutralitätsgebot** beachten (BVerfGE 105, 279, 295). Auch, wenn es im Einzelfall zu Überschneidungen zwischen diesem und dem Sachlichkeitsgebot kommen kann, handelt es sich um unterschiedliche Anforderungen. Das Sachlichkeitsgebot wurde explizit für staatliches Informationshandeln entwickelt, während das Neutralitätsgebot eine grundlegende, übergreifende Pflicht staatlicher Institutionen und deshalb natürlich ebenfalls bei ihrer Öffentlichkeitsarbeit zu beachten ist. Sie müssen unparteiisch sein im Hinblick auf Politik, Weltanschauung und Religion. Sie dürfen sich also "nicht auf eine Seite stellen".

Diese strengen Grenzen bestehen deshalb, weil die Bevölkerung eine erhöhte Sachlichkeits- und Richtigkeitserwartung an die Kommunikation staatlicher Stellen stellt, sobald diese im Kontext ihrer Dienst- und Amtsräume, unter Inanspruchnahme staatlicher Ressourcen oder gar mit öffentlicher Finanzierung agieren. In das Informationshandeln von staatlichen Stellen wird also grundsätzlich besonderes Vertrauen gelegt. Es hat deshalb eine besonders gewichtige Rolle im demokratischen Prozess.

Weiterführende Materialien zu den rechtlichen Grundlagen staatlichen Informationshandelns

- Gusy, Christoph, "Der transparente Staat", in: Hill/Martini/Wagner (Hrsg.), Transparenz, Partizipation, Kollaboration, 2014 zu den Grundlagen staatlicher Öffentlichkeitsarbeit, der aktuellen Gesetzeslage und möglichen Ermächtigungsgrundlagen.
- BVerfG, Beschluss vom 26.06.2002 - 1 BvR 670/91, BVerfGE 105, 279 ("Osho"-Beschluss);
- BVerfG, Beschluss vom 26. 6. 2002 - 1 BvR 558/91 u. a., BVerfGE 105, 252 ("Glykol"-Entscheidung) und
- BVerfG, Beschluss vom 24. 5. 2005 - 1 BvR 1072/01, BVerfGE 113, 63. Diese Gerichtsurteile sind Grundsatzentscheidungen des Bundesverfassungsgerichts, aus denen sich die oben genannten Grundsätze für staatliches Informationshandeln entwickelt haben.

Die Lösungen zu den folgenden praktischen Übungen finden Sie auf den Seiten 178 f.

Fallbeispiel 1

In einer kleinen Stadt verbreitet sich das Gerücht, dass das Trinkwasser kontaminiert sei und zu schweren gesundheitlichen Problemen führen könne. Die Gerüchte führen zu Panik und Hysterie unter den Bürger:innen, welche beginnen, Wasser in Flaschen zu horten. Die örtliche Umweltbehörde, die für die Überwachung der Wasserqualität zuständig ist, erfährt von den Gerüchten und beschließt, eine Gegeninformation zu veröffentlichen, um die Bevölkerung zu beruhigen.

In ihrer Pressemitteilung und auf ihren Social-Media-Kanälen erklärt die Umweltbehörde, dass das Trinkwasser absolut sicher sei und die Gerüchte haltlos und von "unverantwortlichen Panikmachern" verbreitet würden. Die Behörde bezeichnet die Verbreiter der Gerüchte als "gefährliche Lügner" und "Feinde des öffentlichen Friedens". Diese drastische Wortwahl sorgt für Aufsehen und Kontroversen in der Stadt.

Welches Gebot staatlichen Informationshandelns könnte die Umweltbehörde mit ihrer Gegeninformation verletzt haben? Ging die Behörde noch verhältnismäßig vor, indem sie abwertende Aussagen tätigte?

Fallbeispiel 2

In einer Großstadt kursiert in den sozialen Medien das Gerücht, dass es in einem belebten Stadtpark in den letzten Tagen zu mehreren schweren Überfällen gekommen sei. Die Gerüchte schüren Angst und Verunsicherung unter den Bürger:innen, die den Park meiden. Um die Situation zu beruhigen und die Öffentlichkeit zu informieren, veröffentlicht die örtliche Polizeibehörde auf ihrer Website und über ihre Social-Media-Kanäle eine Gegeninformation.

Die Polizei erklärt, dass es in dem betreffenden Zeitraum keine vermehrten Überfälle im Park gegeben habe und dass die Bürger:innen den Park ohne Bedenken nutzen können. Diese Erklärung basiert jedoch auf veralteten Kriminalitätsstatistiken, da die aktuellen Berichte über Vorfälle noch nicht vollständig ausgewertet wurden.

Nach der Veröffentlichung der Gegeninformation stellt sich heraus, dass es tatsächlich mehrere Überfälle gegeben hatte, die den Gerüchten entsprachen. Einige Bürger:innen, die auf die beruhigenden Informationen der Polizei vertrauten, wurden im Park überfallen und erlitten Verletzungen.

Welches Gebot staatlichen Informationshandelns könnte die Polizeibehörde mit ihrer Gegeninformation verletzt haben, indem sie sich auf veraltete Datenbanken stützte?

Die Lösungen zu den folgenden Quizfragen finden Sie auf Seite 180 f.

Frage 1

Welche Aufgabe hat die staatliche Öffentlichkeitsarbeit im Sinne der Kommunikation mit der Bevölkerung?

a) Die Bürger:innen ausschließlich über Sicherheitsmaßnahmen zu informieren.

b) Den Bürger:innen fundierte Informationen bereitzustellen, um sie entscheidungsfähig zu machen.

c) Werbung für politische Parteien zu machen.

Frage 2

Welche Grundbedingung muss staatliche Öffentlichkeitsarbeit erfüllen?

a) Sie muss hauptsächlich auf Unterhaltung abzielen.

b) Sie muss sich ausschließlich im Rahmen des zugewiesenen Aufgaben- und Zuständigkeitsbereichs der jeweiligen staatlichen Stelle bewegen.

c) Sie muss die Interessen der Regierungspartei unterstützen.

Wenn Sie dieses Training alleine absolvieren, nehmen Sie sich fünf bis zehn Minuten Zeit, um über die folgenden Fragen zu reflektieren.

Wenn Sie dieses Training in einer Gruppe absolvieren, reflektieren Sie zunächst 5 Minuten alleine über diese Fragen. Finden Sie sich dann in Zweiergruppen zusammen und diskutieren Sie Ihre Einschätzungen. Diskutieren Sie anschließend im Plenum.

1. Wenden Sie diese Maßnahme (aktive, präventive Kommunikation) in Ihrer Institution an? Wie erfolgt sie (Kanäle, Schwerpunkte, Anlässe)?

2. Was sollte präventiv kommuniziert werden, um Falschinformationen vorzubeugen?

3. Was sind die Grenzen präventiver Kommunikation?

4. Wie groß ist die Aufmerksamkeit der Bevölkerung für präventive Kommunikationsinhalte der BOS? Ist die Aufmerksamkeitsspanne irgendwann "überreizt" und wie lässt sich das verhindern?

5. Welche Vor- und Nachteile verschiedener Herangehensweisen beziehungsweise mögliche Gefahren sehen Sie hier? Was ist Ihnen bei der präventiven Kommunikation wichtig?

Wenn Sie dieses Training alleine absolvieren, nehmen Sie sich fünf bis zehn Minuten Zeit, um über die folgenden Fragen zu reflektieren.

Wenn Sie dieses Training in einer Gruppe absolvieren, reflektieren Sie zunächst 5 Minuten alleine über diese Fragen. Finden Sie sich dann in Zweiergruppen zusammen und diskutieren Sie Ihre Einschätzungen. Diskutieren Sie anschließend im Plenum.

1. Reagieren Sie auf Falschinformationen, die in den sozialen Medien kursieren? Wenn ja, auf welche Art von Falschinformationen (nicht)?

2. Welche Überlegungen spielen bei einer potenziellen Reaktion für Sie eine Rolle?

3. Welche Vorteile sehen Sie darin, auf Falschinformationen zu reagieren? Welche Gefahren bestehen?

4. Wie wirksam sind Gegeninformationskampagnen und Debunking? Wo sind die Grenzen?

5. Werden Ihre Richtigstellungen von den Social-Media-Nutzenden gut akzeptiert? Stoßen bestimmte Formulierungen und Herangehensweisen auf Widerstand und Ablehnung in der Bevölkerung?

6. Gibt es Situationen, in denen Sie bestimmte Informationen nicht oder noch nicht veröffentlichen können, obwohl sie wichtig wären, um Unsicherheiten zu beseitigen und Falschinformationen zu verhindern? Wenn ja, welche Situationen und Gründe sind das?

Wenn Sie dieses Training alleine absolvieren, nehmen Sie sich fünf bis zehn Minuten Zeit, um über die folgenden Fragen zu reflektieren.

Wenn Sie dieses Training in einer Gruppe absolvieren, reflektieren Sie zunächst 5 Minuten alleine über diese Fragen. Finden Sie sich dann in Zweiergruppen zusammen und diskutieren Sie Ihre Einschätzungen. Diskutieren Sie anschließend im Plenum.

1. Wie können Sie sicherstellen, dass Ihre Kommunikation wahrheitsgemäß ist?

2. Wen erreichen Sie durch Ihre Kommunikationsmaßnahmen und wen nicht?

10. Vertrauens- und Communitymanagement

Community- oder Vertrauensmanagement bedeutet, dass BOS sich bemühen, auf ihren Webseiten und Kanälen eine **Community an Follower:innen aufzubauen**, d.h. Menschen, die ihren Veröffentlichungen folgen und/oder dazu Kommentare schreiben. Diese Menschen können BOS gewinnen, indem sie regelmäßig informative, aber auch – wie wir noch problematisieren werden - teilweise humoristische oder rührende Beiträge veröffentlichen. Das Ziel ist zum einen, **Imagepflege** zu betreiben und zum anderen, **Vertrauen** bei den Follower:innen aufzubauen (Jarolimek und Melzer 2022). In Summe sollen mehr Follower:innen für die Kanäle der eigenen Institution gewonnen werden.

Ein solches Communitymanagement kann folgende Vorteile bieten:

- Wenn die Nutzenden mehr Vertrauen und auch Interesse an den Seiten der BOS haben, wird es **wahrscheinlicher, dass sie nicht nur im Alltag, sondern auch in Krisen und Katastrophen die Seiten der BOS** besuchen. Es ist damit auch wahrscheinlicher, dass sie **eher den Informationen der BOS vertrauen und diese aktiv einholen**, als dass sie andere Quellen nutzen (I04).
- Follower:innen sind auch **potenziell Multiplikator:innen**, d.h. Menschen, die die Informationen der BOS an andere weitergeben und sie an anderen Stellen verlinken. Mit mehr Follower:innen erhöht sich die **Reichweite** der BOS, was es in Katastrophenfällen erleichtert, lebenswichtige Informationen zu streuen.
- Teilweise trägt die Community dazu bei, dass **BOS ihrerseits wichtige Informationen erhalten**, z.B. indem sie auf problematische Kommentare, Themen und Trends im Internet hinweist (I06). Gerade in Krisen erhalten Social Media Teams oft so viele Kommentare, dass gerade kleine Teams allein nicht in der Lage wären, diese abzuarbeiten. Eine aktive Community kann beim Social Media Monitoring eine Hilfe sein.
- Die Community hilft zudem oft dabei, **kritische Kommentare oder falsche Informationen auf den Kanälen der BOS zu beantworten** und bei Diskussionen zu **moderieren**. Für BOS kann das von Vorteil sein, da sie dann oftmals nicht mehr selbst reagieren müssen (I01, I06-I08).

10.1 Ethisch-rechtliche Überlegungen

Communitymanagement baut auf einer gelungenen Kommunikation auf. **Die ethischen Überlegungen zu einer guten und ethisch reflektierten Krisenkommunikation** treffen in diesem Sinne natürlich auch auf das Communitymanagement zu (siehe Kapitel 9.2).

Darüber hinaus sollten BOS zwei weitere Aspekte bedenken: Erstens, wie die Follower:innen gewonnen werden und zweitens, wie sie mit diesen umgehen.

10.1.1 Was sollten BOS bei der Gewinnung von Follower:innen beachten?

Um **Follower:innen zu gewinnen, können BOS mehrere Strategien** benutzen: Sie können erstens versuchen, durch möglichst **informative und hochwertige Beiträge** zu überzeugen, also Neuigkeiten von ihrer Institution zu veröffentlichen oder zu Themen aus ihrem Aufgabenbereich zu berichten. Dies ist **aus ethischer Sicht unproblematisch**. Den Bürger:innen stichhaltige Informationen zu liefern, ist sogar ein Ziel guter Behördenkommunikation und liegt im **gesetzlichen Auftrag** staatlicher BOS. Die Bürger:innen können damit eigenständig bessere Handlungsentscheidungen treffen und gewinnen an **Autonomie** (“Selbstermächtigung“; Gusy 2014: 86).

BOS können zweitens **Nahbarkeit demonstrieren**, indem sie einen **persönlichen und emotionalen Kommunikationsstil** pflegen. Das bedeutet, dass sie beispielsweise humorvolle Posts veröffentlichen, berührende Geschichten aus ihrer Arbeit erzählen oder auch Persönlicheres über die Mitarbeitenden zeigen. Auch direkte Antworten auf User:innenfragen oder gute Wünsche zu Feiertagen können dazu beitragen, Follower:innen an sich zu binden. Erfahrungsgemäß werden gerade solche Posts besonders oft angesehen und geliked (W05). Solche nahbaren und persönlichen Beiträge können eine Behörde menschlicher und zugänglicher erscheinen lassen und für **Aufmerksamkeit und einen Vertrauensgewinn** sorgen (vgl. Walsh/O'Connor 2019: 5–6). Dies kann eventuell auch dazu führen, dass **Menschen in Katastrophen oder Krisen sich eher an eine solche nahbare Institution** wenden.

Doch aus ethischer und rechtlicher Sicht birgt diese Strategie auch Nachteile. Zwar erhöht sie die Aufmerksamkeit, die Strategie ist aber durchaus auch “heikel“ (Wagner/Görgen 2018: 63). Behörden haben eine Position der Autorität inne und ihre Kommunikation sollte sachlich und neutral sein. Wenn sie sich von der sachlichen Ebene lösen, besteht immer die **Gefahr, dass ihre Posts als aufmerksamkeitsheischend, salopp oder gar lächerlich** wahrgenommen werden. Die **Jagd nach Likes und Follower:innen ist daher kein Selbstzweck**, sondern das Social Media Team sollte gut abwägen, welches Image ihre Kanäle transportieren.

Auch **rechtlich** gesehen ist diese Strategie heikel: Besonders an staatliche Behörden bestehen **hohe Anforderungen an den Umgang mit der eigenen Onlinepräsenz**. Diese Anforderungen beziehen sich einerseits auf die Moderation der eigenen Onlinepräsenz (siehe Kapitel 11), andererseits aber auch auf die eigene Darstellung, insbesondere, wenn dadurch die Meinungsfreiheit oder Persönlichkeitsrechte der Nutzenden beeinträchtigt werden. Die Rechtsprechung hat daher **Kriterien für staatliche Öffentlichkeitsarbeit und staatliches Informationshandeln** entwickelt (siehe Kapitel 9.4). Diese greifen bereits bei der Kommunikation mit der eigenen Community. Informationen müssen **sachlich und richtig** sein. Und über all dem steht die staatliche **Neutralitätspflicht**; ein Eindruck von Beeinflussung darf nicht entstehen (Eggers 2020: 70). Als neutrale, staatliche Akteure können Behörden nicht wie viele andere Agierende im Netz den gleichen Weg zugespitzter, emotionalisierender Informationen gehen.

10.1.2 Was sollten BOS beim Umgang mit Follower:innen beachten?

Aus ethischer Sicht sollten **Follower:innen** nicht als Unwissende angesehen werden, die es zu belehren gilt. Sie sollten als **freie, gleiche und mündige Bürger:innen, deren Fragen und Beiträge wertgeschätzt** werden, behandelt werden. In einer Demokratie gilt der Grundsatz, dass Menschen möglichst selbst über ihr Leben und ihr Handeln entscheiden können sollten. Behörden sollten die Bürger:innen dabei unterstützen, mit Hilfe guter Informationen und eines respektvollen Dialogs zu eigenen Entscheidungen zu gelangen. Dies ist nur möglich, wenn Behörden den Bürger:innen auf Augenhöhe und als Gleichrangige begegnen (vgl. I09, W01).

BOS bauen mitunter darauf, dass die Followerschaft mithilft, in ihren Kanälen zu moderieren und Falschinformationen richtigzustellen. Dennoch sollten sie die **helfenden Follower:innen nicht als reine Dienstleistende oder Helfer:innen** ansehen. Ihre Mitarbeit ist nicht selbstverständlich. Ethisch gesehen dürfen Menschen **nie als Mittel zum Zweck** benutzt werden, sondern der Mensch und dessen Probleme sollte immer im Blick behalten werden. Daher sollten BOS stets bedenken, dass Follower:innen **Kosten und Nachteile entstehen** können, wenn sie Beiträge verfassen: Sie investieren Zeit und Mühen in die Beiträge, sie treten öffentlich auf und machen sich damit in der Öffentlichkeit angreifbar. Für manche mag es auch psychisch belastend sein, wenn sie sich an kontroversen Diskussionen beteiligen oder einen anderen Post widerlegen (Sievi/Pawelec 2025).

Gegen eine solche **Instrumentalisierung** von Follower:innen zu "Hilfssheriffs" im Netz spricht bei staatlichen BOS zudem aus **rechtlicher Sicht die klare Zuteilung staatlicher Aufgaben**. Unproblematisch ist gewöhnliches Social Media Management, bei dem BOS u.a. die Darstellung eigener Inhalte oder Interaktionsmöglichkeiten mit Posts und User:innen an diesem Ziel orientieren. Die Posts könnten bspw. einladender gestaltet werden, sodass User:innen stärker mit ihnen interagieren. Bei Behörden dient der Internetauftritt häufig aber auch der Erfüllung staatlicher Informationsaufgaben. In dem Fall müssen sie neben den grundsätzlichen Voraussetzungen staatlichen Informationshandelns bei dem Aufbau einer entsprechenden Community darauf achten, die **Grenze zur unzulässigen Übertragung genuin staatlicher Schutzpflichten wie eben der staatlichen Informationstätigkeit nicht zu überschreiten** (ausführlicher zur Informationstätigkeit als staatliche Schutzpflicht siehe Kapitel 9.4).

So darf eine Behörde **Privatpersonen nicht die Ausübung ihrer Informations- und Regulierungstätigkeiten "anvertrauen"**, indem sie sie zur Mitwirkung bei der Erfüllung ihrer hoheitlichen Aufgaben benutzt (Bode 2016: 498). Dies geschieht für gewöhnlich durch Auftragserteilung oder Anstellung. Entsprechend sollten Behörden also **auf monetäre Gegenleistungen oder sonstige Belohnungsmechanismen für ein bestimmtes Verhalten ebenso verzichten, wie auf eine ausdrückliche Auftragserteilung** an die Follower:innen oder Community. Es gilt zudem: Das **letzte Wort behält die Behörde**. Sie muss ihre eigene Onlinepräsenz regelmäßig kontrollieren (bspw. auf rechtswidrige Inhalte) und darf sich n**icht einfach auf eine Selbstregulierung ihrer Community verlassen**, um den vielfältigen, an sie zu stellenden Anforderungen gerecht zu werden (BMI 2014: 23). BOS dürfen im Rahmen des Community Managements darüber hinaus auch **die Nutzbarkeit ihrer Onlinepräsenz als Kommunikationsplattform nicht ungerechtfertigt beschränken**, sollte diese Beschränkung in die Freiheitsrechte der User:innen eingreifen (siehe hierzu ausführlicher Kapitel 11).

Zuletzt sollten sich BOS überlegen, **welche Sprache, welche Inhalte und welche Stilmittel** sie bei ihrem Communitymanagement verwenden. Kanäle, die nur in deutscher Sprache veröffentlicht werden, schließen Menschen aus, die kein Deutsch beherrschen. Doch gerade in Krisen und Katastrophen benötigen solche Menschen ebenfalls überlebenswichtige Informationen. Wird ein Kanal in einer schwer zu lesenden Sprache mit vielen Fremdwörtern und komplizierten Sätzen bespielt, kann dies Menschen unterschiedlicher gesellschaftlicher Schichten und Bildungskreise ausschließen. Auch beim Communitymanagement sollten BOS reflektieren, wie sie mit ihrer Sprache, ihren Inhalten und Stilmitteln möglichst viele Menschen und **unterschiedliche Gruppen erreichen**.

Die Lösungen zu den folgenden Quizfragen finden Sie auf Seite 180.

Frage 1

Was sollten BOS beim Community Management vermeiden, um die Grenze zur staatlichen Aufgabendelegation nicht zu überschreiten?

a) Kommentieren von Beiträgen auf der Pinnwand der eigenen Onlinepräsenz

b) Monetäre Gegenleistungen, Belohnungsmechanismen und ausdrückliche Auftragserteilungen

c) Posten politisch neutraler Imagevideos

d) Liken oder Teilen sachlicher, neutraler und richtiger Inhalte ohne Eingriffscharakter

Frage 2

Wieso muss eine staatliche Behörde ihre Onlinepräsenz im Blick behalten und bei Regulierungsentscheidungen das letzte Wort haben? (2 Antworten richtig)

a) Um kritische Posts im Keim zu ersticken

b) Sie muss auch auf ihrer Social Media Präsenz ihren verfassungs- und verwaltungsrechtlichen Aufgaben gerecht werden können, also etwa die Grundrechte wie die Meinungsfreiheit der Nutzenden schützen und Gefahren für die öffentliche Sicherheit abwehren.

c) Um Diskussionen unter eigenen Beiträgen detailliert zu regulieren

d) Hinsichtlich Beschränkungen von Kommentaren und Nutzenden auf der eigenen Onlinepräsenz muss sie über die Verhältnismäßigkeit des Eingriffs im Einzelfall entscheiden

11. Eskalation

11.1 Grundlagen

Unter der Maßnahme “Eskalation“ fassen wir verschiedene Schritte zusammen, die BOS ergreifen können, wenn sie Desinformationen oder schädliche Inhalte auf digitalen Plattformen identifizieren. Dazu gehört erstens die Meldung verdächtiger Inhalte oder Konten an die Betreiber sozialer Netzwerke (**Meldung an Plattformbetreiber**). Diese sind verpflichtet, solche Meldungen zu prüfen und gegebenenfalls Maßnahmen wie die Löschung oder Einschränkung der Reichweite problematischer Inhalte zu ergreifen. Die Grundlage hierfür bilden rechtliche Regelungen wie das Netzwerkdurchsetzungsgesetz (NetzDG), das Plattformen verpflichtet, rechtswidrige Inhalte zügig zu entfernen oder zu sperren.

Eine **Meldung an Strafverfolgungsbehörden** ist zweitens notwendig, wenn Inhalte nicht nur Desinformationen darstellen, sondern auch gegen Gesetze verstoßen, etwa durch Volksverhetzung, Bedrohungen oder andere Straftatbestände. Solche Maßnahmen sind durch das Strafgesetzbuch (StGB) geregelt, das die rechtlichen Grundlagen für die Verfolgung und Bestrafung solcher Vergehen bietet. Strafverfolgungsbehörden prüfen diese Fälle und leiten juristische Schritte ein, um Täter:innen zur Verantwortung zu ziehen und weiteren Missbrauch zu verhindern. Dies ist ein wichtiger Schritt, um die rechtliche Dimension von Desinformationen zu adressieren und auch um weitere rechtliche Maßnahmen wie Löschung und Blockieren auch durch die Plattformbetreiber selbst zu ermöglichen.

Zu den direkten Maßnahmen, bei denen BOS unmittelbar selbst agieren und nicht “lediglich” der Plattform Meldung erstatten können, zählt drittens auch das **Löschen und Blockieren von Nutzenden und Inhalten** auf den eigenen Kanälen, wenn Plattformbetreiber oder Behörden zu dem Schluss kommen, dass diese gegen geltendes RechtEU-Richtlinien, Verordnungen oder Gesetze verstoßen, oder wenn Behörden von ihrem “digitalen Hausrecht” Gebrauch machen, um etwa die Qualität des Diskurses auf ihren Kanälen zu gewährleisten (siehe Kapitel 11.2). Zumeist können nur Plattformbetreiber Inhalte und Nutzende löschen und blockieren. Grundlage hierfür sind die Plattformregeln sowie gesetzliche Vorgaben wie der Medienstaatsvertrag (MStV) oder das Telekommunikations-Telemedien-Datenschutzgesetz (TTDSG), die Regeln für die Moderation von Inhalten und den Schutz der Nutzendenrechte enthalten. Auf den eigenen Kanälen können jedoch grundsätzlich auch BOS Inhalte, Posts und Nutzende blockieren oder löschen, wobei die **Anforderungen wiederum strenger sind, wenn es sich um staatliche BOS handelt** (siehe Kapitel 11.2).

11.2 Rechtliche und ethische Überlegungen

Die rechtlichen Aspekte dieser Eskalationsmaßnahmen sind komplex und erfordern eine sorgfältige Abwägung zwischen verschiedenen Grundrechten und Rechtsgütern. Aus ethischer Sicht müssen BOS mitunter zwischen widerstreitenden Werten abwägen. Bei der **Meldung an Plattformbetreiber** müssen BOS die Inhalte zunächst prüfen und als potenziell problematisch oder rechtswidrig stufen (OLG Frankfurt a. M. ZUM-RD 2024: 522). Bei der Informationserhebung, die zuvor erfolgen muss, spielen ethische Überlegungen wie Fairness, Nicht-Diskriminierung und Selbstreflexion eine wichtige Rolle (siehe Kapitel 8). Plattformen sind nach dem Netzwerkdurchsetzungsgesetz (NetzDG) dann verpflichtet, solche Hinweise zu bearbeiten. Nach dem Digital Services Act (DSA) werden Meldungen sog. **„vertrauenswürdiger Hinweisgeber“**, zu welchen BOS regelmäßig gehören werden, vorrangig behandelt. Meldungen können dabei von Nutzenden, Organisationen oder staatlichen Stellen eingereicht werden. Diese vertrauenswürdigen Hinweisgeber – oft unabhängige Organisationen oder spezialisierte Einrichtungen – haben gem. Art. 22 DSA das Recht, priorisierte Meldungen über rechtswidrige Inhalte einzureichen. Plattformen müssen diese **Meldungen bevorzugt behandeln und zügig prüfen** (Struzina und Heller 2025: 24). Ziel ist es, die Erkennung und Entfernung von Desinformationen, Hassrede oder anderen illegalen Inhalten effizienter zu gestalten. Damit eine Organisation als vertrauenswürdiger Hinweisgeber anerkannt wird, muss sie nachweisen, dass sie **unabhängig, fachlich qualifiziert und verantwortungsvoll** handelt. Der DSA soll somit sicherstellen, dass legitime Meldungen schnell bearbeitet werden, während gleichzeitig missbräuchliche oder willkürliche Löschungen verhindert werden.

Eine **Meldung an Strafverfolgungsbehörden** wird erforderlich, wenn Inhalte Straftatbestände erfüllen, die etwa im Strafgesetzbuch (StGB) geregelt sind, wie Volksverhetzung (§ 130 StGB) oder Beleidigung (§§ 185 ff. StGB). Solche Meldungen können sowohl von Betroffenen als auch von Behörden oder Dritten veranlasst werden (Walther 2007: 1057).

Die Möglichkeit bzw. unter Umständen auch die Verpflichtung für Plattformbetreiber, Inhalte oder Nutzende zu **löschen oder zu blockieren**, basieren auf Plattformrichtlinien, gesetzlichen Vorgaben des Medienstaatsvertrags (MStV) (wie die Sperrungsvorgaben nach § 109 MStV oder den Vorschriften der Selbstkontrolle gem. § 19 MStV) oder gerichtlichen Anordnungen. BOS hingegen dürfen lediglich im Rahmen ihrer eigenen Online-Präsenz, das heißt auf ihren eigenen Accounts oder Plattformen, löschen und blockieren. Dies wird überwiegend von einer Art **digitalem Hausrecht der BOS** abgeleitet (Eggers 2020: 98). Staatliche Accounts auf Social-Media-Plattformen dienen zudem nicht nur der Informationsvermittlung, sondern bieten auch eine **besondere Plattform für den öffentlichen Diskurs**. Durch ihre offizielle Natur und die damit verbundene Autorität ziehen sie eine breite Öffentlichkeit an und fördern den Austausch zwischen Bürger:innen und Regierung.

Diese Interaktion stärkt die demokratische Teilhabe und ermöglicht es den Bürger:innen, direkt mit staatlichen Stellen zu kommunizieren (Juvan und Svete 2023: 287). Gleichzeitig sind staatliche Stellen verpflichtet, die **Integrität und Qualität dieses Diskurses zu wahren**. Dies beinhaltet die Verantwortung, Beiträge zu moderieren und gegebenenfalls zu entfernen, wenn sie gegen geltende Gesetze verstoßen oder den öffentlichen Frieden gefährden (Eggers 2020: 111 f.). Durch solche Maßnahmen stellen staatliche Accounts sicher, dass ihre Plattformen für einen freien und unbeeinflussten Diskurs genutzt werden können, der den demokratischen Prinzipien entspricht und sich Nutzende nicht aufgrund sog. **Silencing Effekte** dem öffentlichen Diskurs entziehen (Rostalski 2024, 63; Duda et al. 2024: 370). Staatliche BOS nehmen somit eine doppelte Rolle ein – als Fördererinnen des öffentlichen Dialogs und als Hüterinnen der Diskursqualität. Sie bieten nicht nur Informationen, sondern schaffen auch **Räume für Bürgerbeteiligung**, während sie gleichzeitig sicherstellen müssen, dass diese Räume respektvoll und gesetzeskonform bleiben.

Eskalierende Maßnahmen gegen Falschinformationen **berühren jedoch grundlegende Rechte**. So greift das Entfernen oder Blockieren von Inhalten häufig in die **Meinungsfreiheit** (Art. 5 Abs. 1 GG) ein (siehe Kapitel 3). Auch der **Datenschutz** (Art. 2 Abs. 1 GG, Art. 8 EU-Grundrechtecharta) wird berührt, wenn personenbezogene Daten zur Identifikation oder Beweissicherung verarbeitet werden. Zudem könnten Plattformbetreiber Einschränkungen ihrer **Eigentumsrechte** (Art. 14 GG) geltend machen, wenn sie zur Löschung bestimmter Inhalte gezwungen werden.

Obgleich **BOS nur auf ihren eigenen Kanälen Inhalte und Nutzende löschen und blockieren** können, ist dies gerade bei staatlichen BOS bereits eine **sehr invasive** Maßnahme. Hier gelten daher noch strengere Voraussetzungen als bei nicht-staatlichen Institutionen oder den Plattformbetreibern: Die Accounts und Plattformen staatlicher BOS bieten im Gegensatz zu privaten oder nicht staatlichen Accounts einen **besonderen Raum des demokratischen Austauschs** (Eggers 2020: 9 f.). Ein Blockieren oder Löschen muss deshalb noch vorsichtiger gehandhabt werden, als ohnehin schon. Aus ethischer Sicht haben BOS hier eine besondere Verantwortung, die **Meinungsfreiheit** hochzuhalten und insbesondere staatskritische Meinungen nicht aus dem Diskurs auszuschließen. Die **Effektivität dieser speziellen Eskalationsmaßnahme lässt sich deshalb hinterfragen**, kann sie doch nur auf einzelnen Accounts und unter härtesten Voraussetzungen vorgenommen werden.

Insgesamt zeigt sich in der Abwägung, dass eskalierende Maßnahmen tendenziell gerechtfertigt sind, wenn sie im Fall eines Grundrechtseingriffs auf einer gesetzlichen Grundlage basieren und die Grundrechte nicht unverhältnismäßig einschränken. Besonders Maßnahmen, die den Schutz der öffentlichen Sicherheit und der demokratischen Meinungsbildung unterstützen, haben in der Regel ein höheres Gewicht, solange sie transparent und nachvollziehbar umgesetzt werden.

Die Lösungen zu den folgenden Quizfragen finden Sie auf Seite 181.

Frage 1

Welche Voraussetzung muss eine Organisation erfüllen, um als „vertrauenswürdiger Hinweisgeber“ nach dem Digital Services Act (DSA) anerkannt zu werden?

a) Sie muss in staatlichem Auftrag handeln und von der Regierung bestätigt werden.

b) Sie muss unabhängig, fachlich qualifiziert und verantwortungsvoll agieren.

c) Sie muss durch eine richterliche Anordnung als vertrauenswürdig eingestuft werden

Frage 2

Warum gelten für das Löschen und Blockieren von Inhalten durch staatliche BOS besonders strenge Voraussetzungen?

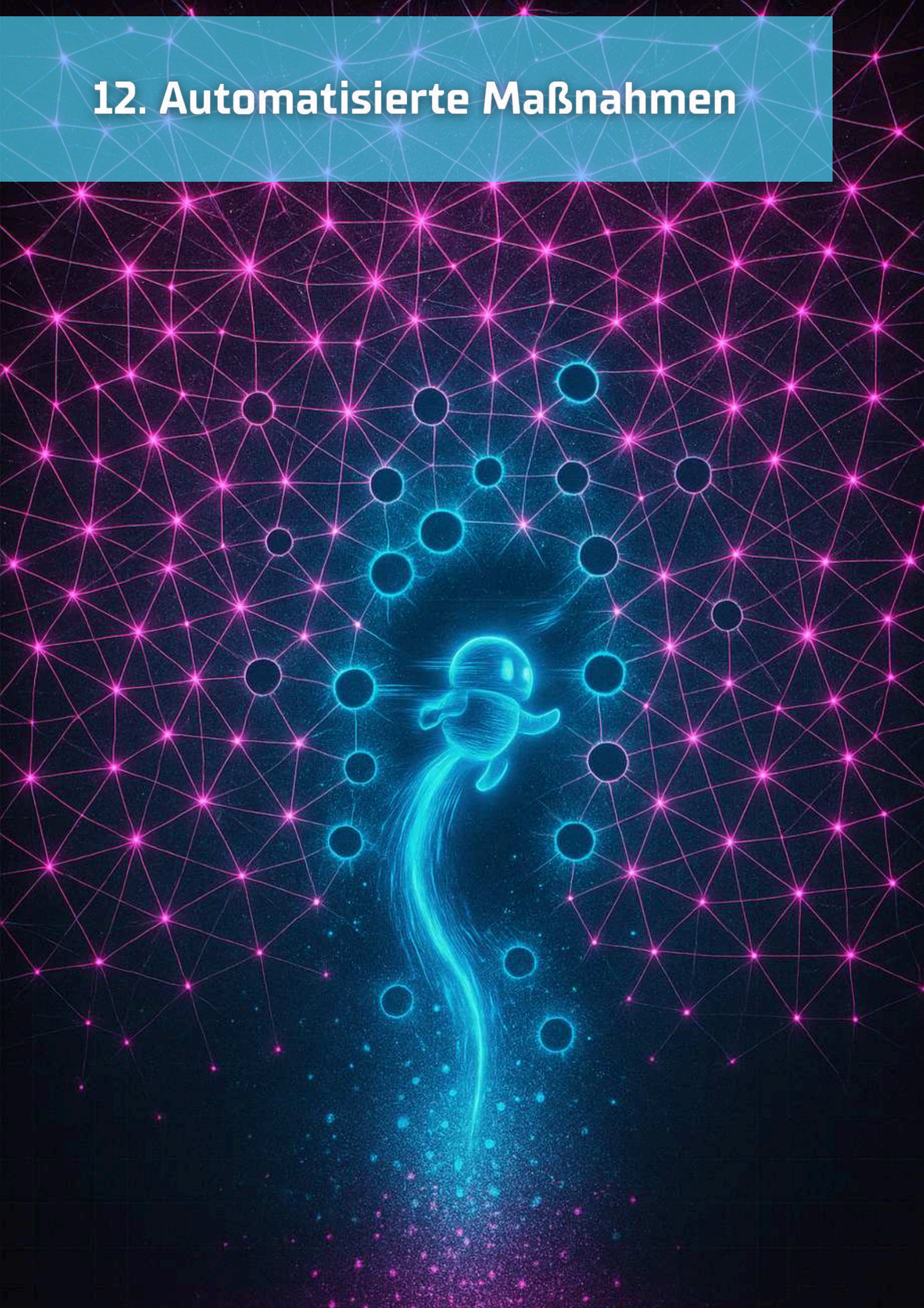
a) Weil ihre Social-Media-Accounts als besondere Plattformen des öffentlichen Diskurses gelten und diese Maßnahmen besonders invasiv sind.

b) Weil staatliche Stellen grundsätzlich keine Inhalte moderieren dürfen.

c) Weil sie bei Löschungen eine richterliche Genehmigung einholen müssen.

d) Weil sie nur Inhalte entfernen dürfen, die bereits durch ein Gericht als rechtswidrig eingestuft wurden.

12. Automatisierte Maßnahmen



12.1 Hintergrund

Die digitalisierte Verbreitung von Falschinformationen birgt neue Risiken und Herausforderungen nicht nur für BOS, sondern insgesamt für die Gesellschaft. Spezifische Herausforderungen für BOS sind neben der Frage der Zuständigkeit (siehe Kapitel 4) im digitalen, internationalen Raum das rasante Tempo der Verbreitung von Falschnachrichten und digitale Besonderheiten wie Anonymität und undurchsichtige Algorithmen der Plattformbetreiber. Diese wiederum verursachen eine enorme Reichweite der Inhalte, ggf. besondere Phänomene wie sog. Filterblasen und Echokammern (deren Existenz allerdings umstritten ist, siehe Kapitel 1.5), und begünstigen die Nutzung von Social Bots, also automatisierten Programmen zur Verbreitung von Inhalten auf sozialen Medien (Fathi et al. 2019: 213). Die besondere Verbreitungsgeschwindigkeit von Falschnachrichten, undurchsichtige Algorithmen und das Geschäftsmodell vieler Plattformen sind zudem Gründe, weshalb Nutzende nicht nur hauptsächlich Inhalte vorgespielt bekommen, welche den eigenen, potenziell ohnehin fälschlichen oder verschwörerischen Ansichten entsprechen und diese dadurch verstärken, sondern auch hauptsächlich solche Quellen frequentieren, die diese widerspiegeln (siehe Kapitel 1.5).

Angesichts rasanter technischer Entwicklungen und neuen Möglichkeiten wie KI-basierter Manipulation wird die Bekämpfung und Prävention von Falschinformationen somit zu einer reinen Sisyphosaufgabe. Was jedoch, wenn man in dem **digitalen Wandel nicht nur die Risiken sieht, sondern auch die Chancen**? Sich neue Verbreitungsmechanismen und technisches Potenzial zunutze zu machen, ist nicht nur den Veröffentlichenden und Verbreitenden von Falschinformationen vorbehalten. Angesichts der rasanten technischen Entwicklungen und Herausforderungen scheint es nötig, dass BOS zumindest in **Betracht ziehen, automatisierte Maßnahmen zu nutzen**, um den enormen Effekt digital verbreiteter Falschinformationen zumindest eindämmen zu können (vgl. I06). Inwiefern dies rechtlich und ethisch vertretbar ist, wird in den vertiefenden Kapiteln aufbereitet. Eine Auswahl solcher Maßnahmen stellen wir Ihnen nachfolgend vor.nittstext

12.2 Worum geht es?

Es stehen mehrere Möglichkeiten zur Verfügung, zumindest in der Theorie Gegenmaßnahmen zu automatisieren. Sie werden in der Wissenschaft diskutiert und in der Praxis teilweise auch angewendet. Allerdings müssen gerade staatliche BOS im Kampf gegen Desinformationen unbedingt die **betroffenen Grundrechte der Nutzenden in verhältnismäßiger Weise berücksichtigen**. Darüber hinaus unterliegt der Einsatz automatisierter Maßnahmen regelmäßig auch **praktischen Grenzen**, weil viele solcher Maßnahmen nur von Plattformbetreibern umgesetzt werden können. Auch **datenschutzrechtliche Anforderungen** sowie solche, die den Einsatz von künstlicher Intelligenz regulieren, müssen BOS zwingend beachten. Darüber hinaus gibt es in Bezug auf den Einsatz automatisierter Maßnahmen teils bedeutende **ethische Bedenken**, etwas wenn Menschen "Entscheidungen" der KI zur Kategorisierung von Falschinformationen und zu ihrer Bekämpfung nicht mehr überprüfen **(menschliche Letztentscheidung)**. Außerdem stellt der **AI Act, die europäische KI-Regulierung**, unter Umständen erhebliche Anforderungen an von BOS genutzte KI-Systeme, abhängig von ihrer Einstufung im risikobasierten Regulierungssystem der EU. BOS müssen sicherstellen, dass ihre Maßnahmen den rechtlichen Vorgaben entsprechen, um Konflikte mit dem AI Act zu vermeiden (hierzu mehr unter Kapitel 12.8). Es ist dabei durchaus möglich, dass potenzielle KI-Anwendungen zur Durchsetzung von Maßnahmen gegen Desinformationen zu der sog. Hochrisiko-KI gehören.

Welche Aufgaben bei der Bekämpfung von Desinformation könnten BOS (teil-)automatisieren? Ist dies aus ethischer und rechtlicher Sicht überhaupt zulässig, und wenn ja, wie sollten BOS es konkret umsetzen? Das können Sie in den folgenden Kapiteln nachlesen, die sich mit den folgenden **Möglichkeiten für BOS** auseinandersetzen:

- **Automatisiertes Social Media Monitoring**
- **Automatisierte Erkennung und Bewertung von Falschinformationen**
- **Automatisierte Bekämpfung von Falschinformationen**
- **Automatisierte Informationsweitergabe und Interaktion mit Bürger:innen**

Dabei werden die einzelnen Automatisierungsmöglichkeiten zunächst (kritisch) beschrieben. Es folgen weiterführende ethische und rechtliche Überlegungen zu den diversen Maßnahmen.

12.3 Automatisiertes Social Media Monitoring

Eine der wichtigsten Präventionsmaßnahmen bei einer eskalierenden Kommunikationskrise ist eine gute Vorbereitung. Diese kann durch automatisiertes Social Media Monitoring unterstützt werden. Monitoring ist auch manuell möglich, indem etwa gezielt nach bestimmten Begriffen gesucht wird (siehe Kapitel 8). Aufgrund der **wachsenden Informationsflut** im Web ist dies jedoch sehr mühsam und zeitaufwendig und es ist fast unmöglich, manuell Diskussionen und wichtige Themen rechtzeitig zu erkennen und zu verfolgen. Dafür müssten enorme personelle und finanzielle Mittel aufgewendet werden, welche häufig nicht zur Verfügung stehen.

Eine automatisierte Informationserhebung kann somit unerlässlich für ein effizientes Monitoring der sozialen Medien sein. Dabei kann sowohl die **Suche nach Inhalten automatisch** stattfinden, als auch die **Analyse** der gefundenen Inhalte (Aßmann und Pleil 2014: 595 ff.). Ziel ist es, wichtige Diskussionen und Kommunikationsmuster zu verfolgen und z.B. mögliche **Krisenherde frühzeitig zu identifizieren und zu analysieren**. Social Media Websites werden dazu mittels automatisiert arbeitender Hilfsprogramme beispielsweise nach **Schlüsselwörtern** durchsucht. Mitunter werden auch alle Nennungen der eigenen Organisation oder alle Inhalte auf den eigenen Kanälen verfolgt, um ein Stimmungsbild in der Bevölkerung zur eigenen Institution oder auch zu einzelnen Einsätzen zu erhalten. Social Media Monitoring Tools arbeiten häufig auch mit einer sogenannten "**Sentiment-Analyse**", also der Einschätzung, ob Posts eher positiv, negativ oder neutral konnotiert sind (Stavrakantonakis et al. 2012: 53, 56). Neben dem Filtern nach bestimmten Inhalten kann KI auch helfen, **aufzudecken, ob hinter bestimmten Profilen Bots** und keine Menschen stecken.

Mithilfe eines automatisierten Social Media Monitorings könnten auch **Falschinformationen schneller herausgefiltert und ihre Ernsthaftigkeit sowie ihr Gefährdungspotenzial bewertet** werden, um darauf basierend rechtzeitig rechtmäßig und ethisch informiert zu handeln (siehe Kapitel 8). Außerdem können BOS den Verlauf der Verbreitung einer Falschinformation beobachten und gegebenenfalls entsprechend die gewählte Handlungsoption anpassen.

Kern des automatisierten Social Media Monitorings ist die Datenerhebung, -aufbereitung und -analyse. Diese Datenverarbeitung wirft unter Umständen nicht nur **datenschutzrechtliche Probleme** auf (siehe Kapitel 5). **Bereits die Erhebung von Daten, um die KI zu trainieren**, kann dahingehend problematisch sein. Besonders kritisch ist zudem die potenzielle Beeinträchtigung von Grundrechten durch Social Media Monitoring durch staatliche Behörden. Durch das im Raum stehende Monitoring des Verhaltens von Nutzenden im Netz entsteht der Eindruck konstanter Beobachtung, wodurch die Nutzenden bewusst oder unbewusst ihr Verhalten und ihre Äußerungen anpassen könnten (also Selbstzensur üben; sog. "**chilling effects**", siehe Kapitel 8). Dies beeinträchtigt sie in ihrer Freiheit und Autonomie, und rechtlich gesehen in ihren Grundrechten der allgemeinen Handlungsfreiheit und der Meinungsfreiheit (GG-Grabenwarter, Art. 5 Abs. 1 Rn. 104). Dabei ist es nicht relevant, ob der/die spezielle Nutzende tatsächlich beobachtet wird. Es reicht, dass durch das grundsätzliche Monitoring durch den Staat eine solche Beobachtung im Raum steht, wodurch Nutzende ihr Verhalten anpassen (Duda et al. 2024: 381).

BOS müssen bei der Anwendung eines automatisierten Social Media Monitoring also datenschutzrechtliche Anforderungen beachten. Sie müssen auch die Beeinträchtigung der Grundrechte von Nutzenden im Einzelfall rechtfertigen können (für eine weitergehende Diskussion siehe Kapitel 8). Die Analyse von Plattforminhalten oder Nutzeraktivitäten muss strikt den **Vorgaben der DSGVO** entsprechen, insbesondere dem Grundsatz der Datensparsamkeit. Eine Erhebung von Daten ohne ausreichende Rechtsgrundlage oder Einwilligung der Betroffenen kann die Privatsphäre ungerechtfertigt verletzen und gegen die DSGVO verstoßen. Beim Social Media Monitoring fehlt häufig eine ausdrückliche Einwilligung, was **rechtliche Unsicherheiten** schafft. Einheitliche Vorgaben für den Umgang mit öffentlich zugänglichen personenbezogenen Daten und ein gemeinsames Verständnis zentraler Begriffe fehlen. Daher ist meist eine Einzelfallprüfung nötig (siehe Kapitel 6). Rechtsgrundlagen wie das öffentliche Interesse gemäß Art. 6 Abs. 1 lit. e DSGVO könnten insbesondere bei behördlicher Nutzung greifen, etwa zur Gefahrenabwehr oder auf Basis polizeilicher Ermächtigungsgrundlagen. Solche Maßnahmen müssen jedoch **verhältnismäßig** sein und Grundrechte wie das **Recht auf informationelle Selbstbestimmung** wahren. Besonders bei der automatisierten Verarbeitung öffentlicher Social-Media-Daten sind rechtliche Grenzen oft unklar, wodurch die Gefahr von Grundrechtsverletzungen steigt. Die DSGVO fordert zudem **Transparenz** über die verarbeiteten Daten und deren Zweck. Ohne ausreichende Anonymisierung und Sicherheitsmaßnahmen bestehen Risiken von Datenschutzverletzungen, was rechtliche und ethische Fragen aufwirft.

12.4 Automatisierte Erkennung und Bewertung von Falschinformationen

Eine Automatisierung des Social Media Monitorings bedingt nicht notwendigerweise, dass die Tools für dieses Monitoring auch Falschinformationen erkennen können. Um der Flut an Falschinformationen im Netz begegnen zu können, ist es jedoch notwendig zu überlegen, die **Erkennung und das Filtern von Falschinformationen** zumindest teilweise zu automatisieren. Dies ist ebenfalls hilfreich für die **Aufdeckung technisch fortgeschrittener Manipulationsmöglichkeiten wie Social Bots und Deepfakes** (siehe Kapitel 1.8).

BOS sollten idealerweise in der Lage sein, Hinweise für eine Manipulation der Inhalte einer Meldung oder für ihre desinformierende Natur automatisiert sammeln zu können. Diese Hinweise können beispielsweise darin bestehen, dass ein Foto bereits in einer früheren Pressemitteilung verwendet wurde und nun **in einem anderen Kontext** verwendet wird, oder dass ein Foto **Spuren einer Bearbeitung** aufweist, die möglicherweise seine Aussage verändert. Bei Texten können etwa Titel, Textkörper und Semantik des Texts – bspw. Emotionen, Stimmung und Thema – zur Untersuchung herangezogen werden (Waidner et al. 2020: 200 ff.; Halvani et al. 2020: 103 ff.; 107 ff.). Bei der Bot-Erkennung geht es um die Frage, ob die Aktivitäten von Nutzenden einer Online-Plattform von Menschen stammen oder ob sie programmgesteuert sind. Wenn hinter den Interaktionen von Profilen ein Computerprogramm steckt, handelt es sich um einen (Social) Bot. Bots haben bspw. eine höhere Neigung, Links zu teilen und Medien (wie Bilder und Videos) häufiger hochzuladen als Menschen (Halvani et al. 2020: 111 f.).

Bei dieser Maßnahme ist zu unterscheiden zwischen **voll- und teilautomatisierten Verfahren**. Bei ersterem verläuft der komplette Vorgang der Erkennung, Bewertung und des potenziellen Downrankings (also der algorithmisch getriebenen niedrigeren Platzierung) von Inhalten ohne menschliche Beteiligung (Jevdenic 2024: 14). Beim teilautomatisierten Verfahren übernehmen Menschen die einzelfallbezogene Interpretation und Überprüfung der von technischen Systemen erzeugten Meldungen. Das System filtert somit nur Inhalte vor, die dann von einem Menschen bewertet werden (**menschliche Letztentscheidung**; Waidner et al. 2020: 200 f.).

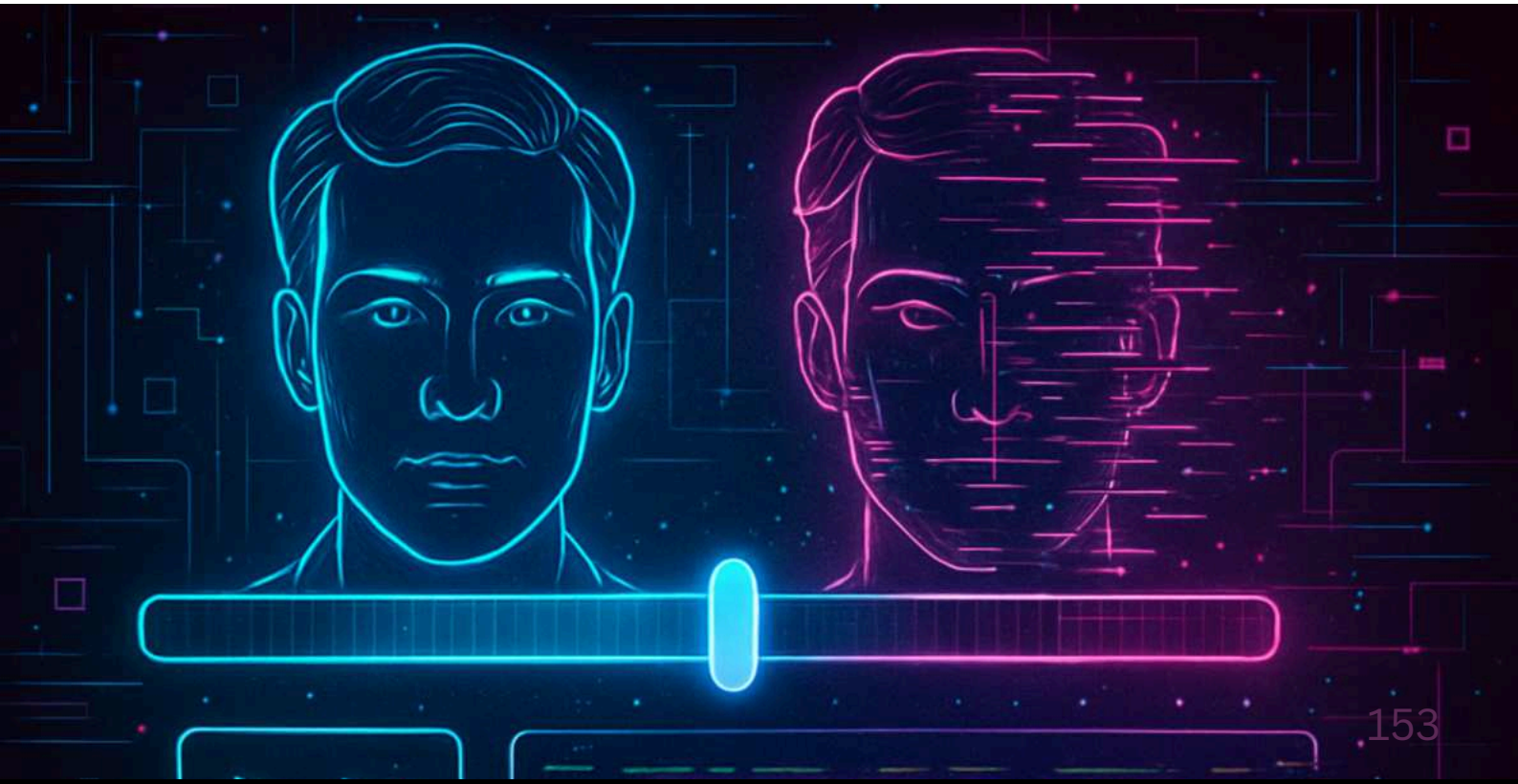
Aus ethischer Sicht sind nur letztere Systeme zulässig, da **automatisierte Maßnahmen auch große Risiken** bergen (siehe Kapitel 12.7). Insbesondere besteht trotz leistungsfähiger KI-Systeme das Risiko **falsch-positiver** Treffer, also von Informationen, die fälschlicherweise als Falschinformationen eingestuft und behandelt werden. Ein KI-System, das autonom agiert, kann dann Entscheidungen treffen, die ungerechtfertigt in einzelne Grundrechte und Werte wie die Meinungsfreiheit eingreifen. Schließlich können technische Systeme **weder den Gesamtzusammenhang eines Inhalts bewerten und damit unterscheiden, ob es sich um eine Tatsachenbehauptung oder eine geschützte Meinungsäußerung** handelt (siehe hierzu Kapitel 3), noch können sie relevante betroffene **Grundrechte und Werte einander gegenüberstellen und abwägen**. Die menschliche Kontrolle und Letztentscheidung KI-basierter Systeme ist also entscheidend.

Doch auch teilautomatisierte Systeme stellen BOS vor technische Herausforderungen: BOS haben **keinen unmittelbaren Zugriff auf diverse Inhalte auf Social Media Plattformen sowie auf deren Verbreitungsmechanismen**. Diesen Zugriff haben nur die Plattformbetreiber. Diese können deshalb einen großen Beitrag zur Falschinformationsbekämpfung und -prävention leisten. Sie können, anders als Außenstehende, auch koordinierte Desinformationskampagnen aufdecken und die Verbreitung schädlicher Inhalte mithilfe algorithmischer Verfahren reduzieren. Viele **Plattformen setzen bereits automatisierte Tools** ein, um unerwünschte Inhalte zu erkennen und zu entfernen. YouTube beispielsweise gibt an, dass von Oktober bis Dezember 2021[4] 99,5% der entfernten Kommentare von automatischen Meldesystemen erkannt wurden. Die anhaltende Debatte über die Gefahr von Falschinformationen in den sozialen Medien zeigt jedoch auf, dass dies keineswegs bedeutet, dass ein substanzieller Anteil der auf YouTube oder anderen Plattformen kursierenden Falschinformationen von den Plattformen aufgedeckt und bearbeitet werden.

[4] *Google*, YouTube-Community-Richtlinien und ihre Anwendung, 2022.

Darüber hinaus ist die automatisierte Erkennung von Falschinformationen technisch eine große Herausforderung. Beispielsweise hinken Tools zur Erkennung von Deepfakes, also manipuliertem oder synthetisch erstelltem Bild-, Video- und Audiomaterial (siehe Kapitel 1.8) der Entwicklung der Deepfake-Technologie grundsätzlich hinterher. Zwar gibt es verschiedenste Ansätze, etwa in der so genannten Bildforensik (also der Untersuchung der Authentizität digitaler Bilder), es handelt sich jedoch um ein "Katz-und-Maus"-Spiel: Immer wenn sich die Deepfake-Detektion entwickelt, wird kurz darauf auch die Generierung von Deepfakes verbessert, um diese Detektion zu umgehen. Dies macht automatisierte Tools zur Erkennung von Deepfakes (ebenso wie solche zur Erkennung von textbasierter Desinformation oder Social Bots) stets anfällig für Fehler. Neben **falsch-positiven** Einschätzungen gehören dazu auch **falsch-negative** Einschätzungen, also, dass manipulierte Inhalte nicht als solche erkannt werden.

Aus rechtlicher und ethischer Sicht dürfen sich **BOS somit nicht blind auf solche Tools verlassen** und ihre Handlungsentscheidungen auf den "Einschätzungen" dieser Formen der künstlichen Intelligenz basieren. Technische Tools müssen für die BOS-Mitarbeitenden erkennbar machen, auf welcher Grundlage sie Einschätzungen über die Echtheit von Informationen bzw. Accounts treffen und wie unsicher diese Aussagen sind (**Transparenz**, Art. 50 AI Act). Es muss dadurch den menschlichen Benutzenden möglich sein, **selbst informierte Entscheidungen zu treffen**; die KI dient dabei nur als **vorab filterndes** Werkzeug.



Inwiefern ein solches Filtern für BOS-Mitarbeitende wirklich hilfreich ist, hängt sowohl von der Güte der technischen Tools als auch vom menschlichen Umgang damit ab. Wenn beispielsweise ein Tool zur Deepfake-Detektion angibt, dass ein Video mit 90-prozentiger Wahrscheinlichkeit gefälscht ist, müssen BOS vorsichtig **abwägen, wie vertrauenswürdig diese Aussage ist und welche Handlungen sie auf dieser Grundlage rechtfertigen** können. Wichtig ist hier aus ethischer Sicht nicht zuletzt, **offen mit eigenen Unsicherheiten und ggf. auch Fehlern umzugehen** und Betroffenen **Widerspruchsmöglichkeiten** einzuräumen. Aus rechtlicher Sicht ergibt sich dies aus rechtlichen Anforderungen wie der DSGVO, die bei automatisierten Entscheidungen menschliche Kontrolle vorschreibt (Art. 22), und dem AI Act, der Transparenz und Nachvollziehbarkeit der Funktionsweise solcher Systeme fordert. KI-Entscheidungen müssen daher offenlegen, wie sie zu ihren Einschätzungen gelangen und welche Unsicherheiten bestehen. Ohne menschliche Kontrolle könnten diskriminierende oder fehlerhafte Entscheidungen getroffen werden, was gegen **Antidiskriminierungsrecht** und Grundrechte verstößt (Langer und Weyerer 2020: 227 f.). Zudem ist die menschliche Überprüfung notwendig, um **Haftungsrisiken** zu minimieren und fundierte, rechtlich abgesicherte Entscheidungen zu gewährleisten.

12.5 Automatisierte Bekämpfung von Falschinformationen

Eine automatisierte Bekämpfung von Desinformation baut auf deren automatisierter Erkennung und Bewertung in Bezug auf deren Risiken auf. Aufgrund der hieraus gewonnenen Erkenntnisse können BOS entsprechende, angemessene weitere Maßnahmen wählen. Dazu könnten auch automatisierte Gegenmaßnahmen gehören, darunter das **automatisierte Ausspielen von Debunking-Nachrichten** über verschiedene Plattformen hinweg (IO6), **Chatbots** zur Interaktion mit Büger:innen (IO5), die **automatisierte Meldung von Falschinformationen an Plattformbetreiber und Strafverfolgungsbehörden**, ein **automatisiertes Löschen oder Blockieren** von Nutzenden oder Inhalten, wobei insbesondere dies erhebliche technische und rechtliche Bedenken aufwirft (siehe Kapitel 11), oder eine **automatisierte Verbreitung von Informationen mittels sog. Social Bots**.

Social Bots sind Computerprogramme, die automatisiert auf Social-Media-Plattformen wie Twitter, Facebook oder Instagram agieren und dabei oft eine menschliche Identität vortäuschen, um ihre Interaktionen glaubwürdiger wirken zu lassen (Stieglitz et al. 2017: 2, 6). Sie können Inhalte posten, auf Beiträge von Nutzenden reagieren oder Diskussionen beeinflussen. Sie werden für verschiedene Zwecke eingesetzt. Einige dienen harmlosen Aufgaben, wie dem automatisierten Teilen von Nachrichten oder Wetterberichten. Andere werden gezielt genutzt, um Meinungen zu manipulieren, Desinformationen zu verbreiten oder Diskussionen zu lenken, zum Beispiel in politischen oder kommerziellen Kampagnen. Problematisch wird der Einsatz von Social Bots, wenn sie den Eindruck erwecken, dass ihre Meinungen von echten Menschen stammen, oder wenn sie massenhaft falsche Informationen verbreiten. Dies kann die öffentliche Meinung verzerren, Vertrauen in Diskussionen schädigen und zu gesellschaftlicher Polarisierung beitragen.

Grundsätzlich ist aber auch **denkbar, dass BOS Social Bots** zur Bekämpfung von Desinformationen nutzen und damit sozusagen eine “behördliche Waffengleichheit” herstellen (Duda et al. 2024: 375). Social Bots können zum Beispiel behördliche Gegeninformationskampagnen vollziehen, bestimmte Äußerungen Einzelner löschen, mit einem Hinweis auf alternative Quellen oder Fact-Checking-Seiten versehen.

Ein weiterer wichtiger Aspekt bleibt allerdings insbesondere bei der automatisierten Bekämpfung von Falschinformationen die **Zusammenarbeit zwischen Mensch und Maschine**. Während Algorithmen effizient große Mengen an Daten durchsuchen können, muss aus ethischer und auch aus rechtlicher Sicht die endgültige Entscheidung über das "Ob" oder "Wie" einer Maßnahme in der Hand von Expert:innen bleiben (**menschliche Letztentscheidung**; siehe Kapitel 12.4). Diese prüfen schwierige Fälle und entscheiden, ob Inhalte tatsächlich Desinformation darstellen und welche Maßnahme geeignet und verhältnismäßig ist. Menschliche Aufsicht ist essenziell, um Fehler und unverhältnismäßige Eingriffe in die Grundrechte von Nutzenden zu minimieren, wie z. B. legitime Inhalte fälschlicherweise als falsch einzustufen. Diese Kombination aus automatisierten Prozessen und menschlicher Aufsicht **erhöht die Zuverlässigkeit, Akzeptanz und Verhältnismäßigkeit** der Maßnahmen (Desoi 2018: 221 f.). Sie trägt dazu bei, **Vertrauen** in die Systeme zu schaffen und **Grundrechte**, wie die freie Meinungsäußerung, besser zu schützen.

12.6 Automatisierte Informationsweitergabe und Interaktion mit Bürger:innen

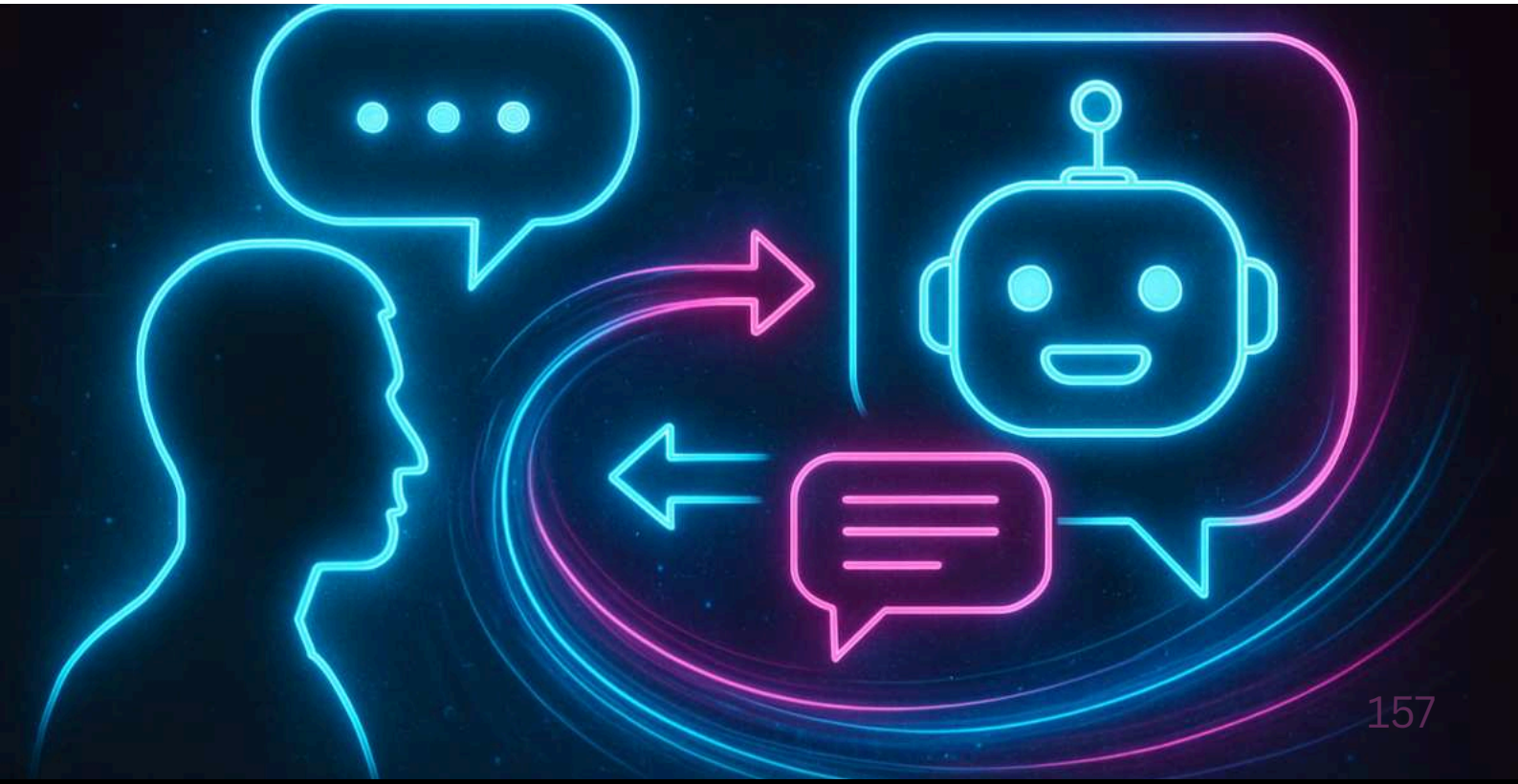
Informationen können in vielen Formen automatisiert an die Bevölkerung weitergegeben werden, um effektiv auf Desinformationen zu reagieren und das Vertrauen in verlässliche Quellen zu stärken. Neben Websites, Social-Media-Plattformen und mobilen Apps könnten BOS auch **digitale Assistenten wie Sprachsteuerungssysteme** (z. B. Alexa oder Google Assistant) oder **Chatbots** nutzen, um auf Bürger:innenanfragen zu aktuellen Themen sofort faktenbasierte Antworten zu liefern (I04, I05). Solche Systeme könnten zudem mit offiziellen Datenbanken verknüpft sein, um stets die neuesten und überprüften Informationen bereitzustellen.

Darüber hinaus könnten **personalisierte Kommunikationswege** eine zentrale Rolle spielen. Behörden könnten mithilfe von Geodaten gezielte Informationen an Menschen in betroffenen Regionen senden, etwa bei Naturkatastrophen oder lokalen Gesundheitsrisiken (Horst 2008: 284). Diese Informationen könnten je nach Medium mit **interaktiven Elementen** ergänzt werden, wie Links zu vertiefenden Inhalten, Videos oder Infografiken, um die Informationen besser verständlich und zugänglich zu machen.

Ein zentraler Erfolgsfaktor für eine solche automatisierte Interaktion mit Bürger:innen ist die **Transparenz** und der **Schutz vor Manipulation**. Nutzende müssen klar erkennen können, dass die Informationen von vertrauenswürdigen Behörden oder Institutionen stammen (Art. 50 AI Act), etwa durch Verifizierungszeichen oder digitale Signaturen. Zudem sollten automatisierte Systeme offenlegen, wie sie arbeiten und welche Quellen sie nutzen. Regelmäßige Überprüfungen und Updates der Systeme sowie Rückmeldungen der Bevölkerung können dazu beitragen, deren Akzeptanz und Effektivität weiter zu steigern (Drewitz et al. 2021: 998). Solche Maßnahmen fördern nicht nur die Verbreitung richtiger Informationen, sondern stärken auch die Resilienz der Gesellschaft gegen Desinformationen.

12.7 Weiterführende ethische Überlegungen zu automatisierten Maßnahmen

Automatisierte Maßnahmen können helfen, damit BOS **trotz begrenzter Ressourcen effektiv gegen Falschinformationen** vorgehen können. Dies kann die **Sicherheit** und gegebenenfalls auch die gesellschaftliche **Gerechtigkeit** erhöhen, wenn beispielsweise Bevölkerungsgruppen über Falschinformationen aufgeklärt werden, die sonst nicht von BOS-Nachrichten erreicht worden wären. Eine automatisierte Beantwortung häufig gestellter Bürger:innenanfragen kann darüber hinaus **personelle Kapazitäten freisetzen**, um auf schwierigere Anfragen und Anliegen einzugehen – oder in der Krise vor Ort Hilfe zu leisten (I04).



Aus ethischer Sicht ist es dabei unerlässlich, dass BOS gegenüber den Bürger:innen **transparent** machen, wann und wofür sie künstliche Intelligenz und andere Formen der Automatisierung einsetzen (IO6). Bürger:innen können sich dann auf ein (teil-)automatisiertes Social Media-Monitoring vonseiten der BOS einstellen. Bei der Interaktion mit BOS-Accounts und Tools im Kontext von Falschinformationen glauben sie zudem nicht fälschlicherweise, dass sie mit einem Menschen interagieren. Diese Transparenz ist ein Wert, der in Überlegungen zur KI-Ethik eine große Rolle spielt.

Doch auch eine klare Kennzeichnung automatisierter Maßnahmen löst nicht alle ethischen Bedenken auf. Die **Erklärbarkeit von Algorithmen** ist ebenfalls ein häufig diskutierter Wert der KI-Ethik: Häufig sind die Algorithmen, die automatisierten Tools zur Informationserhebung, -bewertung und zur Interaktion zugrunde liegen, nicht öffentlich zugänglich und auch für die BOS nicht verständlich. Es handelt sich also um eine sogenannte "Black Box". Auch die **Trainingsdaten**, die den verwendeten Netzen zugrunde liegen, können von BOS meist nicht eingesehen und damit kontrolliert werden.

Daher besteht insbesondere bei der automatisierten Informationserhebung und -bewertung das Risiko, dass verzerrte Algorithmen (mit einem algorithmischen "**bias**", also systematischen Fehlern in der KI, die unfaire oder diskriminierende Folgen haben) zu einer unausgewogenen, diskriminierenden Bewertungen von Informationen kommen und beispielsweise nur Falschinformationen im Blick haben, die aus einem bestimmten politischen Lager stammen (siehe Kapitel 8). Die Erklärbarkeit und Transparenz von Algorithmen ist daher ebenso zentral wie ihre **potenzielle Anpassbarkeit und Beeinflussbarkeit durch die BOS selbst** (Reuter und Kaufhold 2021: 424).

In Bezug auf die Auswirkungen automatisierter Maßnahmen kann ihr Einsatz bis zu einem gewissen Grad eine **Selbstzensur** der Bürger:innen auslösen. Das Wissen, dass Inhalte in den sozialen Medien von staatlicher Stelle aus überwacht und ausgewertet werden, kann Bürger:innen davon abhalten, ihre Meinung kundzutun. Auch der verstärkte Einsatz von **Social Bots kann einer bestimmten Meinung mehr Gewicht geben**, als sie eigentlich im Diskurs hat, und Bürger:innen unter Umständen davon abhalten, ihre Meinung frei zu äußern und sich an politischen Diskussionen zu beteiligen (Möller et al. 2020: 48).

Darüber hinaus bergen automatisierte Lösungen zur Informationsbewertung immer das Problem **falsch-positiver und falsch-negativer Meldungen**, d.h. Informationen werden fälschlicherweise als unrichtig erkannt oder Falschinformationen werden nicht entdeckt. Hier spielt hinein, dass KI, anders als Menschen, nicht über Kontextwissen verfügt, um beispielsweise politische **Satire** als solche zu erkennen. Falsche Einschätzungen können dann den öffentlichen Diskurs sowie die Sicherheit bedrohen und zu einem Verlust von Vertrauen in BOS führen. Darüber hinaus kann eine KI, anders als ein Mensch, **keine einzelfallspezifische Abwägung zwischen widerstreitenden Werten** wie Sicherheit und Meinungsfreiheit treffen. Vollautomatisierte Systeme zur Erkennung und Bekämpfung von Falschinformationen sind aus ethischer Sicht daher abzulehnen. Automatisierte Systeme dürfen vielmehr nur dazu eingesetzt werden, beispielsweise Informationen vorzusortieren und Entscheidungen zu unterstützen. Zentral ist dann die **menschliche Letztentscheidung und Verantwortung (vgl. auch I06)**. Dieser menschlichen Komponente muss **mehr Gewicht verliehen werden, je eingriffsintensiver die automatisierte Maßnahme** ist (bspw. Social Media Monitoring vs. tatsächliches Vorgehen gegen bestimmte Posts).

Eine Herausforderung bergen darüber hinaus **automatisierte Antworten** an Bürger:innenanfragen, die suggerieren, dass sich mit der Anfrage in einem weiteren Schritt ein Mensch beschäftigen wird: Solche Anfragen wecken bei den Bürger:innen mitunter **Erwartungen**, die sich insbesondere in Krisen, in denen zahlreiche Falschinformationen kursieren und die Ressourcen der BOS anderweitig gebunden sind, **nicht erfüllen** lassen. Dies ist vor allem in diesen Situationen für verunsicherte und verängstigte Bürger:innen jedoch kritisch. Eine daraus folgende **Nicht-Antwort** der BOS kann, ebenso wie eine eindeutig nur KI-basierte und **nicht-menschliche Interaktion, das Sicherheitsgefühl der Bürger:innen schmälern**, dazu führen, dass sie sich an weniger verlässliche Quellen wenden, und zu einem **Vertrauensverlust** der Bürger:innen in BOS führen (I05).

12.8 Weiterführende rechtliche Überlegungen zu automatisierten Maßnahmen

Automatisierte Systeme zur Erkennung und Bekämpfung von Falschinformationen dürfen die Meinungsfreiheit nicht unverhältnismäßig einschränken. Das bedeutet, dass sie Inhalte nicht wahllos löschen oder blockieren dürfen. Es sind **spezifische rechtliche Grundlagen** notwendig, um Eingriffe in Grundrechte zu rechtfertigen. Trotz immer leistungsfähigerer Systeme kann das Risiko **falsch-positiver Treffer** in der Regel nicht vollständig ausgeschlossen werden (Ibold 2024: 12). Solche Fehltreffer können beispielsweise satirische Darstellungen sein, die grundsätzlich von der Meinungs- und Kunstfreiheit geschützt sind. Algorithmen können, anders als Menschen, nicht unter Berücksichtigung des Gesamtzusammenhangs der Äußerung zwischen einer Tatsachenbehauptung und einer Meinung unterscheiden. Aufgrund **technikimmanenter Erkenntnisgrenzen** können sie auch nicht wie Menschen den Wahrheitsgehalt einer Tatsachenbehauptung prüfen oder eine Abwägung der widerstreitenden Grundrechtspositionen leisten (siehe hierzu Kapitel 3).

Um Meinungsfreiheit und Demokratie zu schützen, braucht es mehrere abgestimmte Maßnahmen, die rechtliche Vorgaben einhalten. Dabei bedarf es eines **schwierigen Balanceakts mit der Internet(selbst)regulierung**: Einerseits müssen staatliche BOS rechtswidriges Verhalten zugunsten der verhältnismäßigen Freiheitsausübung aller Nutzenden ahnden und regulieren. Andererseits ist es zugunsten gerade dieser Freiheitsausübung der Nutzenden ebenfalls zwingend erforderlich, nicht zu stark einzugreifen, sondern Raum zur Selbstregulierung zu lassen (Christiansen 2000: 126 f., 129). Der Einsatz von KI darf nicht selbst bereits eine Rechtsverletzung bergen (etwa Verstoß gegen das datenschutzrechtliche Verbot automatisierter Einzelentscheidungen) oder herbeiführen (etwa Entfernung eines rechtmäßigen, von der Meinungsfreiheit [Art. 5 Abs. 1 GG] geschützten Beitrags) und Nutzende dürfen zudem nicht in Unkenntnis darüber gelassen werden, **dass und in welcher Art und Weise sie automatisierten Entscheidungen ausgesetzt sind**. Gesetze wie das Netzwerkdurchsetzungsgesetz (NetzDG), weitestgehend abgelöst und erweitert durch das Digitale-Dienste-Gesetz (DDG), und der Medienstaatsvertrag (MStV) sollen helfen, diese Herausforderungen zu bewältigen, indem sie den Plattformbetreibern bestimmte (Transparenz)Pflichten auferlegen.

Jenseits rechtswidriger Äußerungen sind die Aufgaben staatlicher BOS als Exekutivorgane sehr begrenzt. Sie richten sich maßgeblich auf die **Aufrechterhaltung der Bedingungen für die Selbstorganisation gesellschaftlicher Kommunikation** (Pohle und Thiel 2019: 67). Dem Grundsatz der staatlichen Zurückhaltung (Eggers 2020: 70) folgend, greift die Regulierung erst ein, wenn die gesellschaftliche Auseinandersetzung versagt. Dabei schafft sie Rahmenbedingungen für einen fairen Umgang mit KI-Systemen und für Content-Moderation. Maßnahmen wie das Sperren von Konten oder Entfernen von Beiträgen müssen klare, **vorher festgelegte Regeln und verfahrensrechtliche Sicherheiten** haben.

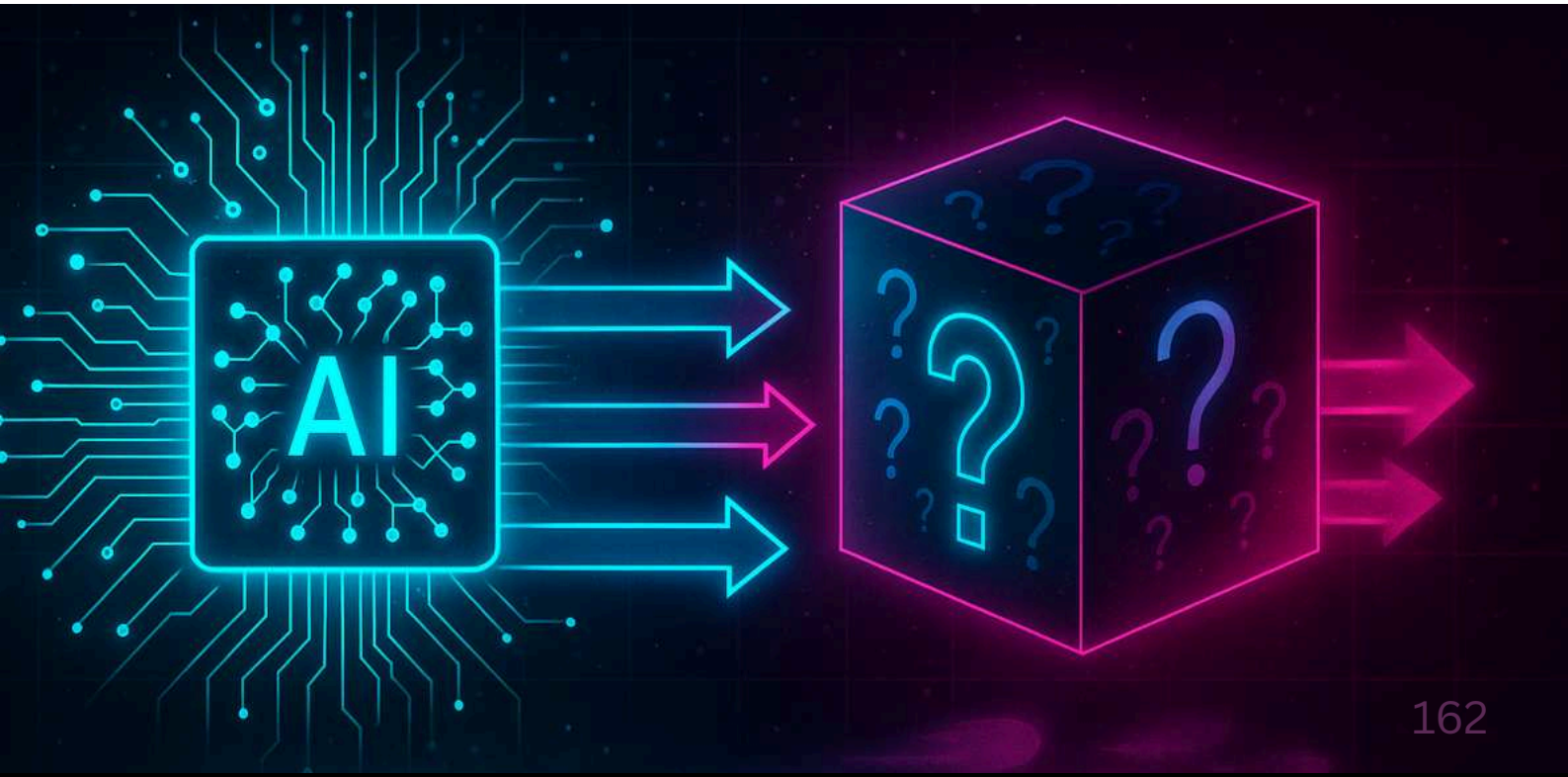
Ein zentraler Aspekt bleibt die **Transparenz und auch die Diskriminierungsfreiheit** des Einsatzes automatisierter Maßnahmen. **Transparenz** bedeutet, dass die (in diesem Fall von BOS) verwendeten Algorithmen, die zugrunde liegenden Daten und deren Verarbeitung nachvollziehbar sein müssen (Art. 50 AI Act), damit die Betroffenen (hier die Nutzenden der sozialen Medien) nachverfolgen können, in welcher Weise und nach welchen Kriterien die genutzte KI auf den freien Diskurs einwirkt und sie potenziell in ihren Grundrechten wie ihre Meinungsfreiheit oder ihr Recht auf Privatsphäre (Art. 1 Abs. 1 i. V. m. Art. 2 Abs. 1 GG) verletzt. Dabei geht es neben Sanktionen, wie das Löschen von Inhalten und das Sperren von Nutzerkonten, um weitere Formen der Content-Moderation, wie die Kennzeichnung oder das – mitunter für Nutzende nicht erkennbare – Downranking von Falschinformationen, bei denen die Verletzung von Grundrechten ebenfalls nicht ausgeschlossen ist. **Diskriminierungsfreiheit** erfordert, dass die Systeme keine ungerechtfertigten Vorurteile gegenüber bestimmten Gruppen oder Individuen perpetuieren, was bestimmte soziale Gruppen benachteiligen könnte. KI-Systeme dürfen also keine unzulässigen Verzerrungen oder Diskriminierungen aufweisen (Legner 2024: 426).

Das bedeutet, dass BOS, die KI einsetzen, regelmäßig im Rahmen des Möglichen und Zumutbaren prüfen müssen, ob die Algorithmen diskriminierungsfrei arbeiten und ob bestimmte Gruppen aufgrund ihrer Merkmale ungerechtfertigt benachteiligt werden. Diese Maßnahmen umfassen etwa die Überprüfung der Trainingsdaten und die der Algorithmen, was deren Transparenz voraussetzt (Legner 2024: 429). Zum Beispiel könnten bei der Klassifizierung von Desinformation bestimmte fehlerhafte Bewertungen, wie falsch-positive Meldungen, auftreten. Bei fehlender Transparenz der Algorithmen besteht die sog. **“Black-Box-Problematik”** (dazu und zu falsch-positiven Meldungen schon Kapitel 12.7).

Um die mit dem Einsatz von KI entstehenden Risiken zu minimieren, sind die Einhaltung gesetzlicher Vorgaben (darunter des EU AI Act, siehe unten), regelmäßige Überprüfungen und die Wahrung von Transparenz und Fairness notwendig. Ein solcher Einsatz von KI muss stets verhältnismäßig sein und die demokratischen Prinzipien der **Rechtsstaatlichkeit und Menschenrechte** respektieren. In der Praxis stellt dies jedoch eine erhebliche Herausforderung für Behörden dar, da ihnen oft die technischen Ressourcen, spezialisierten Fachkräfte oder ausreichende Einblicke in die teils proprietären Algorithmen externer Anbieter fehlen. Insbesondere die Sicherstellung der Transparenz und Nachvollziehbarkeit von Algorithmen kann problematisch sein, wenn diese auf geschlossenen Systemen oder Black-Box-Modellen basieren (Merkle 2024: 416).

Solche Fragen zur **praktischen Umsetzbarkeit** der Anforderungen an diskriminierungsfreie Algorithmen werden sich erst im Laufe der Zeit konkretisieren, da die zugrunde liegenden Vorschriften und Regelungen zur Nutzung von KI in vielen Bereichen noch relativ neu sind. Behörden und andere betroffene Organisationen sammeln derzeit noch Erfahrungen, wie diese Anforderungen technisch, organisatorisch und rechtlich umgesetzt werden können. Gleichzeitig entwickeln sich die Technologien und rechtlichen Standards kontinuierlich weiter, was zusätzliche Anpassungen erforderlich macht. Es ist daher zu erwarten, dass die konkreten Herausforderungen und Lösungsansätze erst mit der Zeit klarer werden.

Bei der Analyse von Informationen greifen automatisierte Systeme zudem häufig auf Daten von Plattformen oder Nutzenden zu. Automatisierte Maßnahmen gegen Desinformationen können mit dem **Datenschutzrecht** kollidieren, wenn sie personenbezogene Daten verarbeiten (siehe hierzu Kapitel 5).

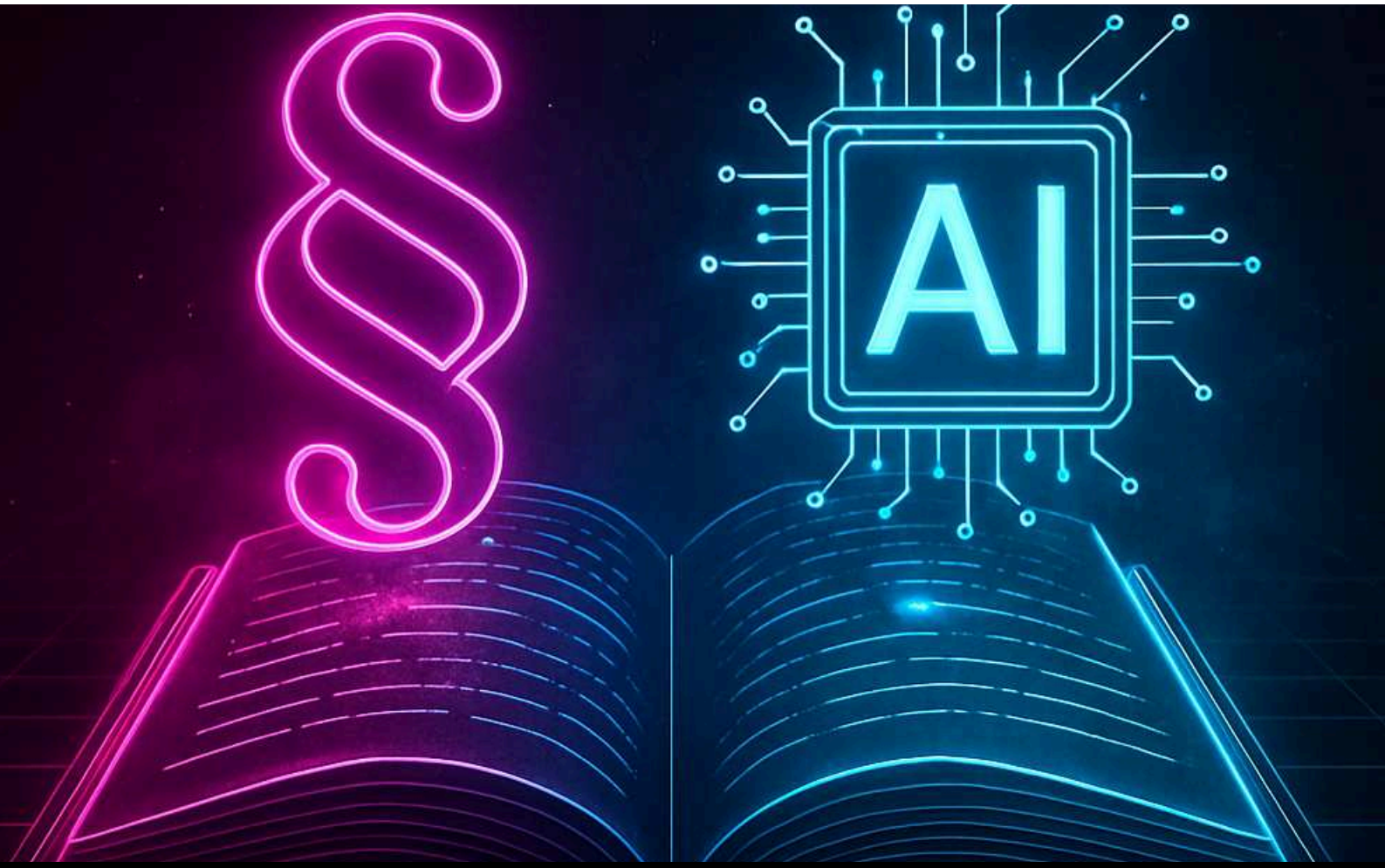


Die Analyse von Inhalten auf Plattformen oder von Nutzeraktivitäten muss den Vorgaben der DSGVO entsprechen, insbesondere dem Grundsatz der Datensparsamkeit. Werden Daten ohne ausreichende Rechtsgrundlage oder Einwilligung erhoben, kann dies die Privatsphäre der Betroffenen in ungerechtfertigter Weise und unter Verstoß gegen die DSGVO verletzen. Beim Social Media Monitoring etwa wird eine explizite Einwilligung im Sinne der DSGVO regelmäßig fehlen. Welche Anforderungen allerdings an eine solche Verarbeitung öffentlich zugänglicher, personenbezogener Daten zu stellen sind, ist aus rechtlicher Sicht nicht abschließend geklärt. Ein gemeinsames Verständnis von zentralen Begrifflichkeiten sowie Vorgaben für den Umgang mit öffentlichen personenbezogenen Daten existieren nicht. Vielmehr bedarf es immer wieder einer **Analyse des Einzelfalls**. Weitere Rechtsgrundlagen wie beispielsweise das öffentliche Interesse (Art. 6 Abs. 1 lit. e DSGVO) könnten insbesondere bei behördlicher Nutzung greifen, etwa bei der Gefahrenabwehr oder im Rahmen der allgemeinen Ermächtigungsgrundlagen in Polizeigesetzen. Solche Eingriffe müssen jedoch immer verhältnismäßig sein und dürfen die Grundrechte, wie das Recht auf informationelle Selbstbestimmung, nicht unverhältnismäßig einschränken. Gerade bei der automatisierten Verarbeitung öffentlicher Daten im Social-Media-Bereich ist die rechtliche Grenze häufig nicht klar definiert, sodass die **Gefahr von Grundrechtsverletzungen** besteht. Zudem erfordert die DSGVO Transparenz darüber, welche Daten verarbeitet werden und zu welchem Zweck. Ohne **angemessene Anonymisierung und Sicherheitsmaßnahmen** besteht das Risiko von Datenschutzverletzungen, was rechtliche und ethische Bedenken aufwirft.

Automatisierte Maßnahmen gegen Desinformationen könnten außerdem in den Anwendungsbereich des sog. **AI Act, also der KI-Regulierung der EU** fallen, da dieser strenge Regeln für KI-Systeme vorsieht. Maßnahmen zur Erkennung oder Blockierung von Desinformationen könnten als **hochriskant** eingestuft werden, da sie die Meinungsfreiheit und den Datenschutz betreffen (Legner 2024: 427). Der AI Act fordert umfassende **Transparenz und Nachvollziehbarkeit** solcher Systeme (Art. 50 AI Act), was zusätzliche Anforderungen an Risikoanalysen und Datensätze bedeutet. Zudem müssen **Diskriminierungsrisiken** vermieden werden, da fehlerhafte oder voreingenommene Algorithmen bestimmte Gruppen benachteiligen könnten (EG 27 AI Act). Bürger:innen müssen außerdem klar erkennen können, wenn KI-Systeme Inhalte überwachen oder analysieren, um die Transparenzpflichten zu erfüllen. Davon betroffen sind etwa Systeme zur Kategorisierung von Personen nach Merkmalen wie Alter, Geschlecht oder ethnischer Zugehörigkeit, Systeme, die in der Strafverfolgung, zur Vorhersage von Straftaten, zur Bewertung von Risikofaktoren oder bei der Analyse von Beweismitteln eingesetzt werden oder auch KI-Systeme, die zur Massenüberwachung verwendet werden, einschließlich der Analyse von öffentlichen Räumen (Art. 6 Abs. 1, Abs. 2, Anhang III AI Act), soweit sie ein “erhebliches Risiko für die Gesundheit, die Sicherheit oder die Grundrechte natürlicher Personen” (also Nutzende) bergen (Art. 6 Abs. 3 AI Act).

Ob und wann von der Kategorie der **Massenüberwachung und der Kategorisierung von Personen** auch Maßnahmen wie das **Social Media Monitoring** erfasst sind, diskutiert die Wissenschaft aktuell noch. Dies ist jedenfalls nicht ausgeschlossen. Die Anforderungen an einen Einsatz künstlicher Intelligenz sind dann unabhängig davon, ob es sich um eine staatliche oder nichtstaatliche Behörde handelt, stark erhöht. Daraus folgende Voraussetzungen für den Einsatz eines solchen KI-Systems wie ein Risikomanagementsystem, die Dokumentation der Entscheidungsprozesse und der eingesetzten Algorithmen zur Rückverfolgbarkeit, Transparenzanforderungen, das Erfordernis menschlicher Überwachung und Kontrolle sowie die Einhaltung gewisser technischer Standards, um Sicherheit und Zuverlässigkeit zu gewährleisten, stellen die Anwender vor **erhebliche organisatorische, finanzielle und personelle Herausforderungen**. Die kann einen solchen Einsatz von KI, hier durch BOS, erschweren bis faktisch kaum umsetzbar machen.

BOS müssen daher sicherstellen, dass ihre Maßnahmen den rechtlichen Vorgaben entsprechen, um Konflikte mit dem AI Act zu vermeiden. Dabei müssen sie nicht nur überprüfen, unter **welche Kategorie** das von ihnen eingesetzte System fällt, sondern auch, ob es ein solches **erhebliches Risiko** für die Gesundheit, die Sicherheit oder die Grundrechte der Nutzenden darstellt. Bei einem Einsatz zur Bekämpfung und Erkennung von Desinformationen wird regelmäßig die Meinungsfreiheit der Nutzenden gefährdet sein. Die Frage ist dann im Einzelfall, ob es sich um eine erhebliche Gefährdung handelt.



Schlusswort

Falschinformationen gefährden nicht nur Einzelne, sondern auch die Integrität von Behörden und die Stabilität demokratischer Gesellschaften. Sie können Grundrechte wie die Meinungsfreiheit, die körperliche Unversehrtheit oder das Recht auf Privatheit beeinträchtigen und in Krisensituationen schwerwiegende Folgen haben. Besonders für Behörden und Organisationen mit Sicherheitsaufgaben (BOS), die für die Sicherheit der Bevölkerung verantwortlich sind, stellt dies eine Herausforderung dar – zum einen, weil sie mit Falschinformationen in verantwortungsvoller und rechtmäßiger Weise umgehen müssen, zum anderen, weil sie selbst Ziel manipulativer Darstellungen werden können.
Zahlreiche Fälle haben in den vergangenen zehn Jahren gezeigt, dass die Verbreitung von Falschinformationen in den sozialen Medien eine immer größere Herausforderung für die Sicherheit und für das Handeln von BOS wird. Gerade angesichts neuer Herausforderungen durch das Aufkommen generativer künstlicher Intelligenz und zunehmend komplexer digitalisierter Desinformationsstrategien ist es entscheidend, dass BOS ihre Verantwortung bewusst wahrnehmen und fundierte Entscheidungen treffen. Die Geschwindigkeit und Reichweite digitaler Falschinformationen erschweren staatlichen Institutionen die rechtzeitige Reaktion und erhöhen das Risiko einer Destabilisierung, insbesondere in Krisenzeiten.

Die vorliegende Handreichung bietet eine erste Orientierung für BOS bei der rechtlichen und ethischen Einordnung bereits ergriffener sowie zukünftig denkbarer Maßnahmen gegen Falschinformationen. Sie soll praktische, wissenschaftlich fundierte Hilfestellungen bieten, aber auch zur Reflexion eigener Werte und Leitbilder sowie zur kritischen Auseinandersetzung mit dem eigenen Handeln anregen. Dabei kann sie keine allgemeingültigen Lösungen liefern. Die Entscheidung über die Wahl passender und rechtmäßiger Gegenmaßnahmen muss stets auf der Grundlage des jeweiligen Einzelfalles getroffen werden. Die Handreichung bietet jedoch wissenschaftlich fundierte Anhaltspunkte und soll zudem zur Anpassung sowie Weiterentwicklung der dargestellten Überlegungen ermutigen.

Wir danken allen Beteiligten, die mit ihrer Expertise und ihren Erfahrungen zu dieser Veröffentlichung beigetragen haben. Wir hoffen, dass diese Handreichung BOS unterstützen wird, rechtssicher und ethisch reflektiert gegen Falschinformationen in den sozialen Medien vorzugehen und dadurch die Sicherheit zu erhöhen, sowie zugleich demokratische Werte und Prinzipien zu wahren und zu stärken.

Lösungen

Fallbeispiel 1

Das Amtsgericht Tiergarten sah in der Formulierung „durchgeknallter Staatsanwalt“ eine Schmähung, die von vornherein nicht zu rechtfertigen sein kann. Eine Abwägung wurde deshalb nicht vorgenommen und der Journalist wegen Beleidigung verurteilt. Das Bundesverfassungsgericht hob die Entscheidung auf. Denn eine nicht mehr abzuwägende Schmähung liegt nicht allein auf Grund der Schwere der Kränkung vor. Hinzu muss kommen, dass die persönliche Kränkung das sachliche Anliegen vollständig in den Hintergrund drängt. Infolgedessen durfte das Amtsgericht den Beschwerdeführer nicht wegen Beleidigung verurteilen, ohne eine Abwägung zwischen seiner Meinungsfreiheit und dem Persönlichkeitsrecht des Geschädigten vorzunehmen.

Fallbeispiel 2

Das Verwaltungsgericht Mainz befand den diffamierenden Gehalt dieser Kommentare für so erheblich, dass sie in jedem denkbaren Zusammenhang als bloße Herabsetzung der Betroffenen erscheinen. Eine Abwägung zwischen dem Grad der Ehrverletzung und dem Recht auf Meinungsäußerung erübrigt sich, da diese Äußerungen nicht mehr als Meinung schützenswert sind. Denn die Bezeichnungen als „fett, alt und hässlich; Untermensch; Drecks-Geschmeiß“ sind hier austauschbare Herabsetzungen, die nicht in einem Bezug zum diskutierten Thema stehen und damit nicht vom Gehalt der Meinung getragen werden können. Wie im Infotext ausgeführt, kann ein Merkmal von Schmähkritiken bzw. Formalbeleidigungen unter anderem dieser fehlende konkrete Sachbezug zur Diskussion sein. Die Folge ist also, dass die Meinungsfreiheit diese Äußerung nicht mehr schützt. Sie wird demnach nicht mehr in die “Waagschale” der Abwägung geworfen. Es bleibt im Ergebnis also nur noch bei der Ehrverletzung der Betroffenen ohne gegenüberstehendes Interesse, welches bei möglichen Maßnahmen berücksichtigt werden müsste. Eine Sperrung des Nutzers auf der eigenen Seite wäre damit legitim, künftig erst Recht eine Meldung in der Position eines Trusted Flaggers nach dem Digital Services Act. Dieser ermöglicht künftig die Priorisierung von Meldungen auf Plattformen durch Nutzend, sofern sie sich nach festgelegten Standards als vertrauenswürdiger Hinweisgeber (“Trusted Flagger”) qualifizieren. BOS erfüllen diese Standards voraussichtlich regelmäßig.

Fallbeispiel 3

Der Vorwurf zielte nicht nur auf das dienstliche Verhalten des Einzelnen, sondern auch allgemein gegen die Ämterführung beim Arbeitsamt, sodass gemäß des Infotexts keine “persönliche Ehre” im eigentlichen Sinne betroffen wurde. Allerdings wurde in der Öffentlichkeit der Eindruck von unlauteren Machenschaften im Behördenapparat erweckt und damit seine Tätigkeit insgesamt herabgewürdigt in einer Weise, bei der seine Funktionsfähigkeit erheblich beeinträchtigt würde.

Die Bundesagentur für Arbeit konnte deshalb gegen den Vorwurf unlauterer Amtsführung einen Unterlassungsanspruch geltend machen. Dies war jedoch nicht zuletzt nur wegen der Drohung, die Behauptung öffentlich zu machen, möglich, denn durch diese Drohung bestand Wiederholungsgefahr (Extrawissen: Das ist eine erforderliche Grundvoraussetzung für einen zivilrechtlichen Unterlassungsanspruch).

Quiz 1

d)

Der richtige Umgang mit Falschinformationen ist eine schwierige Einzelfallentscheidung, zu den Details wird auf den Infotext verwiesen. Eine Erfüllung der Beleidigungsdelikte alleine berechtigt nicht automatisch zur Löschung der entsprechenden Inhalte. Sie können immer noch von der Meinungsfreiheit geschützt sein, da sie einen Beitrag zum geistigen Meinungskampf in einer die Öffentlichkeit wesentlich berührenden Frage darstellen. Je bedeutender dann die Diskussion für die Öffentlichkeit ist, desto eher kann die Meinungsfreiheit ehrverletzende Äußerungen rechtfertigen. Werturteile sind wiederum insgesamt grundsätzlich von der Meinungsfreiheit gedeckt und auch Polemik steht dem nicht entgegen. Die Schutzwürdigkeit von erwiesenen oder bewusst unwahren Tatsachenbehauptungen ist hingegen in der Regel nicht gegeben oder tritt jedenfalls regelmäßig zurück.

Quiz 2

a), c)

Auch hier ist immer eine Betrachtung der Inhalte im Einzelfall relevant. Unter den im Infotext und den Fallbeispielen dargestellten Umständen sind eine strafrechtliche Anzeige, ein zivilrechtlicher Unterlassungsanspruch oder auch ein presserechtlicher Gegendarstellungsanspruch möglich. Da Behörden allerdings neutral und sachlich reagieren müssen, sind polemische Gegenangriffe verfehlt. Auch haben Behörden nicht die Kompetenz, Nutzende auf der gesamten genutzten Plattform zu blockieren, das können nur die Plattformbetreiber. Diese Möglichkeit haben sie aber auf ihren eigenen Kanälen.

Quiz 1

b)

Das Bundesamt für Verfassungsschutz ist für die Überwachung von Desinformation außerhalb der Gefahrenabwehr im Einzelfall zuständig. Es analysiert die Methoden und Mechanismen staatlich gesteuerter Desinformationskampagnen und berichtet darüber an Parlament, Regierung und Öffentlichkeit. Die Polizei ist hingegen nur dann zuständig, wenn eine konkrete Gefahr für die öffentliche Sicherheit oder eine strafbare Handlung vorliegt. Die Bundesnetzagentur ist im Rahmen des Digital Services Acts für die Regulierung digitaler Plattformen zuständig, aber nicht für geheimdienstliche Bedrohungen. Das Bundesamt für Sicherheit in der Informationstechnik beschäftigt sich mit Cybersicherheit, insbesondere mit technischen Bedrohungen wie Hacking oder Cyberangriffen, nicht aber mit gezielten Desinformationskampagnen.

Quiz 2

a)

Ordnungsbehörden haben die Aufgabe, die öffentliche Sicherheit und Ordnung auf kommunaler Ebene zu schützen. Wenn eine lokale Falschmeldung beispielsweise falsche Informationen über eine Bombendrohung oder gefährliche Zustände auf einer Veranstaltung verbreitet, kann die Behörde Auflagen gegen Veranstalter:innen erteilen oder Maßnahmen zur Berichtigung der Information ergreifen. Antwort b) ist falsch, da Streitigkeiten zwischen Privatpersonen in der Regel zivilrechtlich geklärt werden müssen und nicht in den Zuständigkeitsbereich der Ordnungsbehörde fallen. Im Falle strafrechtlicher Relevanz können sie der Zuständigkeit von Polizeibehörden unterfallen. Antwort c) ist ebenfalls nicht korrekt, da überregionale oder internationale Desinformationskampagnen eher in den Zuständigkeitsbereich von Nachrichtendiensten oder spezialisierten Behörden wie dem BKA oder BfV fallen. Antwort d) betrifft keine unmittelbare Gefahrenlage, weshalb eine Ordnungsbehörde nicht zuständig wäre.

Quiz 3

c)

Die Bundesnetzagentur fungiert als Digital Services Coordinator (DSC) für Deutschland und ist somit für die Umsetzung des Digital Services Act (DSA) verantwortlich. Dieser verpflichtet digitale Dienste und Online-Plattformen dazu, Maßnahmen gegen illegale Inhalte und Desinformation zu ergreifen. Plattformen müssen etwa Falschmeldungen kennzeichnen oder entfernen, wenn sie gegen rechtliche Vorgaben verstoßen. Antwort a) ist falsch, da das BSI für technische IT-Sicherheit zuständig ist, aber nicht für die Regulierung von Online-Plattformen. Antwort b) ist nicht korrekt, da das BKA nur bei strafrechtlich relevanter Desinformation ermittelt, aber keine Plattformregulierung vornimmt. Antwort d) trifft nicht zu, weil das BfV zwar ausländische Einflussnahme beobachtet, aber keine regulatorischen Maßnahmen gegenüber Online-Diensten durchsetzen kann.

Fallbeispiel 1

Bei der Analyse von Social Media-Kommentaren muss zunächst geprüft werden, ob ein Personenbezug gemäß Art. 4 Nr. 1 DSGVO vorliegt. Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Eine Person gilt bereits dann als identifizierbar, wenn sie direkt oder indirekt, insbesondere durch Zuordnung zu einer Kennung wie einem Namen, einer Kennnummer, Standortdaten oder zu spezifischen Merkmalen ihrer Identität identifiziert werden kann.

Auch wenn in diesem Fall keine direkten personenbezogenen Informationen wie Namen oder E-Mail-Adressen erfasst werden, kann ein Personenbezug dennoch vorliegen. Dies wäre dann der Fall, wenn die Kommentare zusammen mit Metadaten wie IP-Adressen, Zeitstempeln (also die genaue Uhrzeit und das Datum, zu denen bestimmte Aktionen im Zusammenhang mit einem Social Media-Account erfolgen) oder Nutzernamen gespeichert werden und eine Identifizierung durch Verknüpfung mit anderen Informationen ermöglicht wird. Selbst wenn die Daten anonym erscheinen, besteht die Möglichkeit einer indirekten Identifizierbarkeit, etwa durch Rückschlüsse aus dem Inhalt der Kommentare oder durch eine Analyse über längere Zeiträume hinweg.

Um den Personenbezug zu vermeiden oder zu reduzieren, könnten Maßnahmen wie Anonymisierung oder Pseudonymisierung in Betracht gezogen werden. Bei der Anonymisierung werden alle Merkmale entfernt, die eine Identifizierung ermöglichen, sodass eine betroffene Person nicht mehr bestimmbar ist und die Verarbeitung nicht mehr den Anforderungen der DSGVO unterliegt. Pseudonymisierung hingegen ersetzt identifizierende Merkmale bspw. durch einen Code, sodass die Daten nur mit zusätzlichem Wissen wieder einer Person zugeordnet werden können. Letzteres bietet den Vorteil, dass die Daten unter Einhaltung strenger Schutzmaßnahmen weiterhin genutzt werden können, ohne dass eine direkte Zuordnung ohne zusätzliche Informationen möglich ist. Zugleich reduziert sie “lediglich” datenschutzrechtliche Risiken. Die DSGVO und ihre Anforderungen bleiben anwendbar.

Fallbeispiel 2

Die Verarbeitung personenbezogener Daten im Rahmen der Öffentlichkeitsarbeit kann gemäß Art. 6 Abs. 1 lit. e DSGVO zulässig sein, wenn sie zur Wahrnehmung einer Aufgabe im öffentlichen Interesse oder zur Ausübung öffentlicher Gewalt erforderlich ist. Das öffentliche Interesse allein reicht jedoch nicht aus; es bedarf einer konkreten Rechtsgrundlage im Unions- oder nationalen Recht. In Deutschland stellt § 3 BDSG eine solche Grundlage dar, da er die Datenverarbeitung durch öffentliche Stellen zur Erfüllung von Aufgaben im öffentlichen Interesse regelt. Die Behörde muss zunächst prüfen, ob die geplante Maßnahme tatsächlich unter die Aufgaben der Ordnungsverwaltung fällt, beispielsweise indem sie zur Aufrechterhaltung der öffentlichen Sicherheit und Ordnung beiträgt. Da die Aufklärung über Desinformation das öffentliche Vertrauen in staatliche Institutionen fördern kann, könnte die Maßnahme als eine im öffentlichen Interesse liegende Aufgabe angesehen werden.

Jedoch ist eine Einzelfallprüfung erforderlich, um die Erforderlichkeit und Verhältnismäßigkeit der Datenverarbeitung sicherzustellen. Es muss nachgewiesen werden, dass die Verarbeitung personenbezogener Daten – etwa durch Nennung von Nutzernamen – geeignet und erforderlich ist, um das Ziel zu erreichen, und dass mildere Mittel, wie die anonyme Darstellung von Falschinformationen, nicht ausreichen.

Besonderes Augenmerk muss auf den Anwendungsbereich der DSGVO gelegt werden. Nach Art. 2 Abs. 2 DSGVO findet die Verordnung keine Anwendung auf Tätigkeiten, die der Strafverfolgung oder Gefahrenabwehr dienen. Sollte die Maßnahme jedoch überwiegend präventiven oder strafverfolgungsbezogenen Charakter haben, greift die DSGVO nicht, sondern vielmehr die Richtlinie (EU) 2016/680 oder nationale Gesetze.

Zusammenfassend kann die Behörde personenbezogene Daten im Rahmen der Öffentlichkeitsarbeit verarbeiten, sofern eine konkrete Rechtsgrundlage vorliegt, die Maßnahme verhältnismäßig ist und die DSGVO anwendbar bleibt. Andernfalls sind spezifische Rechtsvorschriften für Sicherheitsbehörden zu beachten.

Quiz 1

b)

Antwort a) ist falsch, weil eine Zweckänderung der Datenverarbeitung (z.B. von Strafverfolgung zu präventiver Polizeiarbeit) grundsätzlich einen neuen Grundrechtseingriff darstellt. Eine solche Änderung erfordert eine neue rechtliche Grundlage, da die ursprüngliche Verarbeitung nicht mehr die gleiche Zielsetzung verfolgt. Antwort c) ist ebenfalls falsch, weil die DSGVO strenge Regeln für die Zweckbindung und die Erforderlichkeit einer neuen Rechtsgrundlage bei einer Zweckänderung vorsieht. Die Zulässigkeit einer Zweckänderung ist nicht allein vom öffentlichen Interesse abhängig, sondern muss eine klare gesetzliche Grundlage haben.

Quiz 2

b)

Auch Standortdaten und technische Kennungen wie IP-Adressen können als personenbezogene Daten gelten, wenn sie mit anderen Informationen verknüpft werden können, die eine Identifizierung der betroffenen Person ermöglichen. Nach der DSGVO kann ein Datenbestand dann als personenbezogen gelten, wenn er direkt oder indirekt eine Person identifizierbar macht. Hierzu zählen auch technische Daten wie IP-Adressen oder Standortdaten, insbesondere wenn sie mit anderen Informationen (z.B. Nutzerverhalten oder Social-Media-Profile) kombiniert werden, um Rückschlüsse auf die betroffene Person zu ziehen. Antwort a) ist falsch, weil ein Personenbezug nicht nur dann vorliegt, wenn Daten direkt auf eine Einzelperson hinweisen. Auch indirekte Identifizierungen, etwa durch die Kombination von Standortdaten oder technischen Kennungen mit anderen Informationen, können zu einem Personenbezug führen. Antwort c) ist ebenfalls falsch, da personenbezogene Daten nicht nur sensible oder private Informationen betreffen. Auch öffentlich zugängliche Daten wie Social-Media-Posts können personenbezogen sein, wenn sie in Verbindung mit anderen Daten eine Identifizierung der Person ermöglichen.

Quiz 3

a)

IP-Adressen und Zeitstempel sind personenbezogene Daten, da sie unter Berücksichtigung zusätzlicher Informationen zur Identifizierung einer Person verwendet werden können, auch wenn diese nicht unmittelbar durch die Behörde erfolgt. Nach Art. 4 Nr. 1 DSGVO gelten auch indirekte Identifikatoren wie IP-Adressen als personenbezogen, wenn sie mit weiteren Daten kombiniert eine Identifizierung ermöglichen. Es reicht aus, dass eine Identifizierung durch Dritte möglich ist, unabhängig von der Absicht der Behörde. Antwort b) ist falsch, weil IP- Adressen als personenbezogene Daten gelten können, wenn sie mit anderen Informationen kombiniert werden. Antwort c) ist falsch, da die Absicht der Identifizierung nicht ausschlaggebend für die Anwendbarkeit der DSGVO ist – entscheidend ist die Möglichkeit der Identifikation.

Quiz 1

a), b)

Medienkompetenztrainings – insbesondere dann, wenn sie von staatlichen Stellen angeboten werden – erreichen voraussichtlich keine Bürger:innen, die staatlichen Behörden und Institutionen und den „Mainstream-Medien“ misstrauen. Sie können keine tiefgreifenden politischen Gräben überwinden. Antwort c) ist daher falsch.

Quiz 2

b)

BOS haben eine besondere Verantwortung, alternative Meinungen und staatskritische Medien nicht zu unterdrücken oder bestimmte Gruppen per se negativ darzustellen. Sie dürfen staatliche Quellen nicht generell oder ausschließlich als vertrauenswürdig und nicht-staatliche Quellen als nicht vertrauenswürdig einstufen. Daher scheidet Antwort a) aus. Auch Antwort c) stimmt nicht: Dies ist zwar wichtig, damit Medienkompetenztrainings Wirkung entfalten. Es ist aber nicht wichtig, um die Demokratie zu stärken.

Quiz 3

b)

Private, nichtstaatliche Einrichtungen haben das Recht, eigenständig die Vermittlung von Medienkompetenz vorzunehmen. Geht es allerdings um die Fragen der Hauptverantwortung und möglichst überprüfbarer und regulierbarer inhaltlicher Richtigkeit und Expertise, liegt das Hauptaugenmerk bei Schulen und Einrichtungen der Erwachsenenbildung. Aufgrund der Schutzpflichten des Staates gegenüber seiner Bevölkerung hat zwar auch dieser eine Hauptrolle bei der Vermittlung von Medienkompetenz. Allerdings liegt die Kompetenz hierfür bei Kindern und Jugendlichen neben der vorrangigen elterlichen Sorge bei den Ländern und damit bei den Schulen. Aufgrund bestehender Ressourcen und Expertise sind ebenfalls im Erwachsenenalter spezialisierte Einrichtungen vorzugswürdig.

Quiz 4

b)

Die Eltern haben gem. Art. 6 Abs. 2 S. 1 GG das Recht und die Pflicht, für ihre Kinder zu sorgen. Dies umfasst die Aufgaben, sie zu beaufsichtigen, zu schützen und zu erziehen. Das gilt auch mit Blick auf die Nutzung digitaler Medien. Antwort a) ist falsch. Zwar steht es den Ländern gem. Art. 7 Abs. 1 GG zu, durch ihre Schulträgerschaft die Medienkompetenzbildung anzubieten. Das letzte Wort und die Hauptverantwortung liegen aber bei den Eltern: Gem. Art. 6 Abs. 2 S. 1 GG haben sie das Recht und die Pflicht, für ihre Kinder zu sorgen. Auch Antwort c) kommt nicht in Betracht. Zwar liegt beim Staat die Hauptverantwortung für die Vermittlung von Möglichkeiten zur Medienkompetenzbildung und die entsprechenden Initiativen. Das Vorrecht der Erziehung, des Schutzes und der Beaufsichtigung von Kindern und Jugendlichen liegt aber bei den Eltern.

Quiz 5

a)

Die Literatur rät dazu, dass der „Angriff“ mit einer Falschinformation schnell nach der Warnung erfolgen sollte, um Verwirrung zu vermeiden. Somit ist Antwort b) ausgeschlossen. Antwort c) ist nicht zutreffend. BOS sollten lieber auf fiktive und unpolitische Beispiele zurückgreifen, um politisch neutral zu bleiben, keine automatischen Abwehrreaktionen bei den Bürger:innen auszulösen, und nicht selbst unbeabsichtigt eine Quelle von Desinformation zu werden.

Quiz 6

c)

Antwort a) entfällt. Diese Sorge ist berechtigt, wenn BOS auf bestimmte Lebensweisen oder politischen Einstellungen verweisen. Sie können jedoch bedenkenlos demokratische Werte und Regeln betonen, die sich ein demokratisches Gemeinwesen gegeben hat. Antwort b) ist ebenfalls nicht möglich. Nudges können beispielsweise in eigenen Social Media Posts gesetzt werden und sind damit nicht besonders ressourcenintensiv.

Quiz 1

b)

Antwort a) ist falsch, weil Social Media Posts zwar grundsätzlich öffentlich sind, BOS allerdings nicht anlasslos personenbezogene Daten verarbeiten und den Eindruck ständiger Beobachtung vermitteln. Antwort c) scheidet ebenfalls aus. Soziale Medien sind zumindest teilöffentlich. Anders sieht es mit privaten Textnachrichten und anderen Inhalten aus, die über Messengerdienste geteilt werden.

Quiz 2

b), c)

Grundsätzlich kann es gerechtfertigt sein, wenn BOS die sozialen Medien nach bestimmten Themen und Suchbegriffen durchsuchen, die für ihre eigene Arbeit und die Sicherheit der Bevölkerung wichtig sind. Allerdings dürfen sie nicht anlasslos und unverhältnismäßig breite Teile der Bevölkerung überwachen. Außerdem müssen sie darauf achten, insbesondere den Datenschutz zu wahren. Zudem schont eine enge Konzentration Ressourcen und vermeidet die Gefahr einer zu breiten Überwachung und von Zuständigkeitsfragen. Allerdings kann sie angesichts der Sicherheitsrelevanz von Falschinformationen in den sozialen Medien auch zu kurz greifen. Gegen Antwort a) spricht, dass Social Media-Kommunikation zu einem gewissen Grad öffentlich ist. Eine Abwesenheit von BOS und Ignoranz der Entwicklungen und Inhalte in den sozialen Medien wäre auch aufgrund der Relevanz der sozialen Medien für gesellschaftliche und politische Diskussionen auch demokratietheoretisch nicht zu rechtfertigen.

Fallbeispiel 1

- Die Umweltbehörde handelt im Rahmen ihrer Zuständigkeit, um die Bevölkerung über die Sicherheit des Trinkwassers zu informieren. Eine grundlegende Voraussetzung ist somit erfüllt.
- Öffentlichkeitsarbeit muss darüber hinaus den Geboten der Richtigkeit, Sachlichkeit und Verhältnismäßigkeit entsprechen.
- Die Umweltbehörde hat korrekt informiert, dass das Trinkwasser sicher ist. Dem Gebot der Richtigkeit wurde damit Genüge getan. Jedoch ist die Frage, ob die Wortwahl ("unverantwortliche Panikmacher", "gefährliche Lügner", "Feinde des öffentlichen Friedens") sachlich und verhältnismäßig war, kritisch zu prüfen.
- Dem Gebot der Sachlichkeit zur Folge müsste die Behörde wertungsfrei vorgehen. Dies wurde durch die Verwendung der abwertenden Aussagen unterlassen, die Informationsverbreitung ist inhaltlich und auch in ihrer Darstellung äußerst (negativ) wertend.
- Mit der Veröffentlichung sind auch Nachteile für Betroffene verbunden, jedenfalls werden ihre Persönlichkeitsrechte berührt. Die Inhalte müssten sich also auf das zur Informationsgewährung Erforderliche beschränken. Erforderlich ist ein Inhalt, wenn kein milderes, gleich geeignetes Mittel zur Zielerreichung ersichtlich ist. In diesem Fall wäre die Informationsverbreitung mindestens genauso effektiv, wenn nicht sogar effektiver, weil sie nicht antagonistisch verbreitet worden wäre, wären die abwertenden Bezeichnungen unterblieben. Das Vorgehen ist somit unverhältnismäßig.

Fallbeispiel 2

- Die Polizei handelt im Rahmen ihrer Aufgaben zur Gefahrenabwehr und zur Gewährleistung der öffentlichen Sicherheit.
- Öffentlichkeitsarbeit muss den Geboten der Richtigkeit, Sachlichkeit und Verhältnismäßigkeit entsprechen.
- Da die Abwehr dringender Gefahren häufig schnelles Handeln unter den Bedingungen unvollständiger Sachverhaltskenntnis erfordert, müssen staatliche BOS die zeitlich mögliche Sachverhaltsaufklärung leisten. Angesichts der akuten Bedrohung für die körperliche Unversehrtheit der Bürger:innen aufgrund des kurzfristigen, erhöhten Vorkommens in der spezifischen Gegend wäre eine hinreichende Überprüfung notwendig gewesen. Es wäre durchaus möglich und zumutbar gewesen, die aktuellen Kriminalitätsstatistiken einzusehen, bevor man eine Entwarnung aussprach. Dies ist ebenfalls Ausfluss des Gebots der Richtigkeit, sodass die Polizei dieses missachtet hat.

Quiz 1

b)

Staatliche Öffentlichkeitsarbeit soll die Bürger:innen im demokratischen Sinne möglichst fundiert entscheidungsfähig machen, damit sie an der politischen Willensbildung im demokratischen Prozess teilhaben können. Die Öffentlichkeitsarbeit ist nicht ausschließlich auf Sicherheitsmaßnahmen beschränkt, sondern erfasst alle staatlichen Politikbereiche. Sie darf aber natürlich keine Werbung für politische Parteien machen.

Quiz 2

b)

Eine Grundbedingung für die Zulässigkeit der staatlichen Öffentlichkeitsarbeit ist, dass sie sich im Rahmen des zugewiesenen Aufgaben- und Zuständigkeitsbereichs der jeweiligen staatlichen Stelle bewegt. Da sie der Information der Bevölkerung im Rahmen des demokratischen Prozesses dient, ist ihr Unterhaltungsfaktor kein relevanter Aspekt. Ebenso widerspräche es dem Neutralitätsgebot staatlicher Einrichtungen, müssten sie die Interessen einer bestimmten Partei stützen.

Quiz 1

b)

Unproblematisch ist gewöhnliches Social Media Management, das die Grundsätze staatlicher Sachlichkeit, Neutralität und Richtigkeit nicht überschreitet. Problematisch wird die Interaktion mit den eigenen Follower:innen vor allem dann, wenn ureigene staatliche Aufgaben wie Informations- und Regulierungstätigkeiten faktisch auf die Nutzenden übertragen werden.

Quiz 2

b), d)

Antwort a) ist falsch: Die Onlinepräsenzen staatlicher Behörden dienen nicht nur dem eigenen Social Media Auftritt, sondern sind zugleich auch eine bedeutsame Plattform für den demokratischen Austausch der Bevölkerung. Es muss ein Balanceakt geführt werden zwischen dem Schutz der Grundrechte der Nutzenden sowie der öffentlichen Sicherheit und der Ermöglichung einer möglichst unbeeinflussten Diskussion. Bereits kritische Posts im Keim zu ersticken oder eine über detaillierte Regulierung von Diskussionen unter eigenen Beiträgen, ginge in der Regel zu weit. Auch Antwort c) ist nicht korrekt. Die Onlinepräsenzen staatlicher Behörden dienen nicht nur dem eigenen Social Media Auftritt, sondern sind zugleich auch eine bedeutsame Plattform für den demokratischen Austausch der Bevölkerung. Es muss ein Balanceakt geführt werden zwischen dem Schutz der Grundrechte der Nutzenden sowie der öffentlichen Sicherheit und der Ermöglichung einer möglichst unbeeinflussten Diskussion. Bereits kritische Posts im Keim zu ersticken oder eine über detaillierte Regulierung von Diskussionen unter eigenen Beiträgen, ginge in der Regel zu weit. Antwort d) ist richtig: Die Onlinepräsenzen staatlicher Behörden dienen nicht nur dem eigenen Social Media Auftritt, sondern sind zugleich auch eine bedeutsame Plattform für den demokratischen Austausch der Bevölkerung. Es muss ein Balanceakt geführt werden zwischen dem Schutz der Grundrechte der Nutzend sowie der öffentlichen Sicherheit und der Ermöglichung einer möglichst unbeeinflussten Diskussion. Bereits kritische Posts im Keim zu ersticken oder eine über detaillierte Regulierung von Diskussionen unter eigenen Beiträgen, ginge in der Regel zu weit.

Quiz 1

b)

Sie muss unabhängig, fachlich qualifiziert und verantwortungsvoll agieren. Der DSA verlangt von vertrauenswürdigen Hinweisgebern, dass sie unabhängig arbeiten und über nachgewiesene Fachkompetenz verfügen. Dies dient dazu, die Qualität und Neutralität der gemeldeten Inhalte sicherzustellen. Antwort a) und c) sind falsch, weil weder eine staatliche Beauftragung noch eine richterliche Anordnung erforderlich sind. Die Vergabe des Status als vertrauenswürdiger Hinweisgeber erfolgt auf Antrag und nach Prüfung durch den Koordinator für digitale Dienste. In Deutschland ist dies die Bundesnetzagentur.

Quiz 2

a)

Weil ihre Social-Media-Accounts als besondere Plattformen des öffentlichen Diskurses gelten. Staatliche Accounts dienen der demokratischen Meinungsbildung und ermöglichen den Bürger:innen direkte Kommunikation mit staatlichen Stellen. Eingriffe in diesen Diskurs erfordern daher eine besonders strenge Abwägung. Staatliche Stellen dürfen Inhalte moderieren, jedoch nur unter strengen Voraussetzungen.

Andı, Simge/Akesson, Jesper (2021). **Nudging Away False News: Evidence from a Social Norms Experiment**. Digital Journalism 9 (1), 106–125. https://doi.org/10.1080/21670811.2020.1847674.

Bäcker, Matthias (2021): **B. Die Polizei im Verfassungsgefüge**. In: Hans Lisken und Erhard Denninger (Hg.): Handbuch des Polizeirechts. Gefahrenabwehr - Strafverfolgung - Rechtsschutz. München.

Barczak, Tristan (2023a): **§ 1 Zentrale Einrichtungen zur Zusammenarbeit in kriminalpolizeilichen Angelegenheiten**. In: Tristan Barczak (Hg.): BKAG. Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten. 1. Aufl. Baden-Baden.

Barczak, Tristan (2023b): **§ 5 Abwehr von Gefahren des internationalen Terrorismus**. In: Tristan Barczak (Hg.): BKAG. Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten. 1. Aufl. Baden-Baden.

Bartlett, Jamie/Miller, Carl/Crump, Jeremy/Middleton, Lynne (2013). **Policing in an Information Age**. CASM policy paper. Online verfügbar unter https://demos.co.uk/wp-content/uploads/files/DEMOS_Policing_in_an_Information_Age_v1.pdf (abgerufen am 02.02.2024).

BeckOK InfoMedienR-Söder (1.11.2024). In: BeckOK Informations- und Medienrecht. 46. Aufl.

BfV (2023): **Desinformation als Mittel gezielter Einflussnahme fremder Staaten**. Online verfügbar unter https://www.verfassungsschutz.de/SharedDocs/hintergruende/DE/spionage-und-proliferationsabwehr/desinformation.html#:~:text=in%20unmittelbare%20Kriegshandlungen.xn--,Was%20ist%20und%20wie%20wirkt%20Desinformation%3F,Verbreiten%20falscher%20oder%20irrefhrender%20Informationen-lol., zuletzt geprüft am 23.04.2025.

BMBF (2022). **Forschung gegen Fake News. Desinformation verstehen, erkennen, bekämpfen**. Online verfügbar unter chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.bmbf.de/SharedDocs/Publikationen/DE/L/31723_Forschung_gegen_Fake_News.pdf?__blob=publicationFile&v=4 (abgerufen am 20.02.2025).

BMI (2014). **Leitfaden Krisenkommunikation**. Online verfügbar unter https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/bevoelkerungsschutz/leitfaden-krisenkommunikation.pdf?__blob=publicationFile&v=4 (abgerufen am 07.03.2025).

Bode, Lorenz (2016). **Der Einsatz privater Sicherheitsdienste aus verfassungsrechtlicher Perspektive**. Neue Justiz, 497–499.

boyd, danah (2018a). **A Few Responses to Criticism of My SXSW-Edu Keynote on Media Literacy**. Online verfügbar unter https://zephoria.medium.com/a-few-responses-to-criticism-of-my-sxsw-edu-keynote-on-media-literacy-7eb2843fae22 (abgerufen am 20.03.2024).

boyd, danah (2018b). **You Think You Want Media Literacy... Do You?** Data & Society. Online verfügbar unter https://www.zephoria.org/thoughts/archives/2018/03/09/you-think-you-want-media-literacy-do-you.html (abgerufen am 05.02.2024).

BSI (2025): **Wahlen in Deutschland 2025. Bedrohungslage umfasst Desinformation, Verfügbarkeitsangriffe und Cyberspionage**. Online verfügbar unter https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Analysen-und-Prognosen/Threat-Intelligence/Krisen-Grosslagen/Wahlen/wahlen_node.html, zuletzt geprüft am 23.04.2025.

Buchner, Benedikt/Petri, Thomas (2024). In: Datenschutz-Grundverordnung/BDSG. Kommentar. 4. Aufl. München.

Christiansen, Per (2000). **Selbstregulierung, regulatorischer Wettbewerb und staatliche Eingriffe im Internet**. MMR, 123–129.

Dederer, Hans-Georg (2024): Art. 35. In: Günter Dürig, Roman Herzog und Rupert Scholz: Grundgesetz Kommentar. 105. EL.

Desoi, Bernd Uwe (2018). **Big Data und allgemein zugängliche Daten im Krisenmanagement. Exemplarische technische und normative Gestaltung von Analysen zur Entscheidungsunterstützung**.

Drewitz, Uwe/Wilbrink, Marc/Oehl, Michael/Jipp, Meike/Ihme, Klas (2021). **Subjektive Sicherheit zur Steigerung der Akzeptanz des automatisierten und vernetzten Fahrens**. Forschung im Ingenieurwesen 85, 997–1012.

DS-GVO/BDSG-*Hansen* (2025). In: Datenschutzrecht. DS-GVO/BDSG. 2. Aufl. Baden-Baden.

DS-GVO-*Heberlein* (2024). In: Datenschutz-Grundverordnung Kommentar. 3. Aufl. München.

DS-GVO-*Klabunde/Horváth* (2024). In: Datenschutz-Grundverordnung Kommentar. 3. Aufl. München.

DS-GVO BDSG-*Pötters* (2022). In: Datenschutz-Grundverordnung VO (EU) 2016/679 Bundesdatenschutzgesetz Kommentar. 3. Aufl.

DS-GVO BDSG-*Schulz* (2022). In: Datenschutz-Grundverordnung VO (EU) 2016/679 Bundesdatenschutzgesetz Kommentar. 3. Aufl.

Duda, Michelle/Evans, Alison/Rostalski, Frauke (2024). **Fake News mit Social Bots bekämpfen? Zur Zulässigkeit des behördlichen Einsatzes von Social Bots im Umgang mit Falschnachrichten**. Zeitschrift für Digitalisierung und Recht (4), 365–390.

Duden (2025). **Shitstorm, der**. Online verfügbar unter https://www.duden.de/rechtschreibung/Shitstorm (abgerufen am 07.02.2025).

Dunckel, Till (2020). **Der rechtliche Rahmen der Verwaltungskommunikation**. In: Klaus Kocks/Susanne Knorre/Jan Niklas Kocks (Hg.). Öffentliche Verwaltung – Verwaltung in der Öffentlichkeit. Wiesbaden, Springer Fachmedien Wiesbaden, 57–75.

Eccles, David A./Dingler, Tilman (2021). **Three prophylactic interventions to counter fake news on social media**. HI '21 Extended Abstracts in the Proceedings of the Workshop on Technologies to Support Critical Thinking in an Age of Misinformation (CTAM21),. Online verfügbar unter https://arxiv.org/ftp/arxiv/papers/2105/2105.08929.pdf (abgerufen am 21.02.2024).

Eccles, David A./Kurnia, Sherah/Dingler, Tilman/Geard, Nicholas (2021). **Three Preventative Interventions to Address the Fake NewsThree Preventative Interventions to Address the Fake News Phenomenon on Social Media**. Online verfügbar unter https://aisel.aisnet.org/acis2021/51/.

Eggers, Christian W. (2020). **Quick Guide Social-Media-Recht der öffentlichen Verwaltung. Rechtliche Grundlagen und Gestaltungsoptionen in der Öffentlichkeitsarbeit**. Wiesbaden.

Fathi, Ramian/Brixy, Anne-Marie/Friedrich, Frank (2019). **Desinformationen und Fake-News in der Lage: Virtual Operations Support Team (VOST) und Digital Volunteers im Einsatz**. In: Hans-Jürgen Lange/Michaela Wendekamm (Hg.). Postfaktische Sicherheitspolitik. Gewährleistung von Sicherheit in unübersichtlichen Zeiten. Wiesbaden/Heidelberg, Springer VS, 211–235.

Fechner, Frank (2023). **Medienrecht. Lehrbuch des gesamten Medienrechts unter besonderer Berücksichtigung von Presse, Rundfunk und Multimedia**. 22. Aufl. Stuttgart.

Gabel, Friedrich/Krüger, Marco (2020). **Leitfaden für eine ethisch reflektierte Krisenkommunikation: eine Analyse wertbezogener Spannungsfelder in der Krisenkommunikation**. Internationales Zentrum für Ethik in den Wissenschaften (IZEW), Universität Tübingen. Tübingen. Materialien zur Ethik in den Wissenschaften. Online verfügbar unter https://uni-tuebingen.de/de/81680 (abgerufen am 20.02.2024).

GG-*Badura* (2024). In: Grundgesetz Kommentar. 105. Aufl. Bd. 1.

GG-*Grabenwarter* (2024). In: Grundgesetz Kommentar. 105. Aufl. Bd. 1.

GG-*Paulus* (2024). In: Grundgesetz Kommentar. 8. Aufl. München.

GG-*Rixen* (2024). In: Grundgesetz Kommentar. 10. Aufl. München.

Gimpel, Henner/Heger, Sebastian/Olenberger, Christian/Utz, Lena (2021). **The Effectiveness of Social Norms in Fighting Fake News on Social Media**. Journal of Management Information Systems 38 (1), 196–221. https://doi.org/10.1080/07421222.2021.1870389.

Gusy, Christoph (2014). **Der transparente Staat**. In: Hermann Hill (Hg.). Transparenz, Partizipation, Kollaboration. Die digitale Verwaltung neu denken. Baden-Baden, 81–93.

Halvani, Oren/Freifrau Heeremann von Zuydtwyck, Wendy/Herfert, Michael/Kreutzer, Michael/Lui, Huajian/Simo Fhom, Hervais-Clemence/Steinebach, Martin/Vogel, Inna/Wolf, Ruben/Yannikos, York/Zmudzinski, Sascha (2020). **Automatisierte Erkennung von Desinformationen**. In: Martin Steinebach/Katarina Bader/Lars Rinsdorf et al. (Hg.). Desinformationen aufdecken und bekämpfen. Interdisziplinäre Ansätze gegen Desinformationskampagnen und für Meinungspluralität. Baden-Baden, 101–148.

Hamann, Christian/Klar, Manuel/Wegmann, Simon (2023). **§ 8 Datenschutzrecht**. In: Eric Wagner/Moritz Holm-Hadulla/Marc Ruttloff (Hg.). Metaverse und Recht. München.

*Hong, Mathias (*2022). **Hassrede und Desinformation als Gefahr für die Demokratie - und die Meinungsfreiheit als gleiche und positive Freiheit im Zeitalter der Digitalisierung**. Rechtswissenschaft (1), 126–174.

Horst, Bruno (2008). **Internetbasierte Kommunikationskonzepte**. In: Hardy Geyer/Uwe Manschwetus (Hg.). Kulturmarketing. München, 279–292.

Ibold, Victoria (2024). **Künstliche Intelligenz im Sicherheitsrecht - Begründungsgebot quo vadis?** Zeitschrift für das Gesamte Sicherheitsrecht, 10–18.

Jarolimek, Stefan/Melzer, Anne (2022). **Öffentliche Kommunikation, Polizei und Corona**. In: Hans-Jürgen Lange (Hg.). Politik zwischen Macht und Ohnmacht. Wiesbaden, Springer Fachmedien Wiesbaden, 341–361.

Jevdenic, Rade (2024). **Governance von Social-Media-Algorithmen. Analyse der Aufsicht und Regulation**. Chur.

Juvan, Jelena/Svete, Uroš (2023). **Die Nutzung sozialer Medien in den Streitkräften von heute - ein gemischter Segen**. In: Eva Moehlecke de Baseggio/Olivia Schneider/Tibor Szvrircsev Tresch (Hg.). Soziale Medien und die Streitkräfte, 283–300.

Kuhlmann, Simone; Trute, Hans-Heinrich (2022): **Die Regulierung von Desinformationen und rechtswidrigen Inhalten nach dem neuen Digital Services Act**. In: GSZ, S. 115–122.

Kunig, Philip/Berger, Ariane (2021). In: Grundgesetz Kommentar. 7. Aufl. Bd. 1. München.

Langer, Paul/Weyerer, Jan (2020). **Diskriminierungen und Verzerrungen durch Künstliche Intelligenz. Entstehung und Wirkung im gesellschaftlichen Kontext**. In: Michael Oswald/Isabelle Borucki (Hg.). Demokratietheorie im Zeitalter der Frühdigitalisierung. Wiesbaden, 219–240.

Legner, Sarah (2024). **KI-Verordnung und algorithmische Diskriminierung**. Recht Digital, 426–432.

Lewandowsky, Stephan/Ecker, Ullrich K. H./Seifert, Colleen M./Schwarz, Norbert/Cook, John (2012). **Misinformation and Its Correction: Continued Influence and Successful Debiasing**. Psychological science in the public interest: a journal of the American Psychological Society 13 (3), 106–131. https://doi.org/10.1177/1529100612451018.

Loh, Wulf (2021). **Soziale Medien**. In: Michael G. Festl (Hg.). Handbuch Liberalismus. Berlin/Heidelberg, J.B. Metzler, 543–551.

Lu, Chang/Hu, Bo/Li, Qiang/Bi, Chao/Ju, Xing-Da (2023). **Psychological Inoculation for Credibility Assessment, Sharing Intention, and Discernment of Misinformation: Systematic Review and Meta-Analysis**. Journal of medical Internet research 25, e49255. https://doi.org/10.2196/49255.

Mafi-Gudarzi, Nima (2019). **Desinformation: Herausforderung für die wehrhafte Demokratie**. Zeitschrift für Rechtspolitik, 65–68.

Martins Geraldes, Sofia (2023). **Die dunkle Seite der Interkonnektivität: Soziale Medien als Cyberwaffe?** In: Eva Moehlecke de Baseggio/Olivia Schneider/Tibor Szvrircsev Tresch (Hg.). Soziale Medien und die Streitkräfte, 235–256.

Mason, Lance E./Krutka, Dan/Stoddard, Jeremy (2018). **Media Literacy, Democracy, and the Challenge of Fake News**. Journal of Media Literacy Education 10 (2), 1–10. https://doi.org/10.23860/JMLE-2018-10-2-1.

McDougall, Julian (2019). **Media Literacy versus Fake News: Critical Thinking, Resilience and Civic Engagement**. Media Studies 10 (19), 29–45. Online verfügbar unter https://hrcak.srce.hr/ojs/index.php/medijske-studije/article/view/8786.

Merkle, Marieke Luise (2024). **Transparenz nach der KI-Verordnung - von der Blackbox zum Open-Book?** Recht Digital, 414–420.

Milborn, Corinna/Punz, Magdalena (2022). **Dr. Lisa-Maria Kellermayr: Eine Würdigung**. Puls24 vom 30.07.2022. Online verfügbar unter https://www.puls24.at/meinung/dr-lisa-maria-kellermayr-eine-wuerdigung/271669?utm_source=pocket-newtab-global-de-DE (abgerufen am 27.02.2024).

Möller, Judith/Hameleers, Michael/Ferreau, Frederik (2020). **Typen von Desinformation und Misinformation. Verschiedene Formen von Desinformation und ihre Verbreitung aus kommunikationswissenschaftlicher und rechtswissenschaftlicher Perspektive**. Online verfügbar unter https://www.lfk.de/fileadmin/PDFs/Publikationen/Studien/Typen-von-Desinformation-und-Misinformation/typen-von-desinformation-und-misinformation.pdf (abgerufen am 10.01.2025).

Mols, Frank/Haslam, S. Alexander/Jetten, Jolanda/Steffens, Niklas K. (2015). **Why a nudge is not enough: A social identity critique of governance by stealth**. European Journal of Political Research 54 (1), 81–98. https://doi.org/10.1111/1475-6765.12073.

Müller, Stephan (2024). **20. Frankfurter Medienrechtstage 2024. Strategien gegen Desinformation und Propaganda**. Neue Justiz (5), 216–219.

Norri-Sederholm, Teija/Norvanto, Elisa/Talvitie-Lamberg, Karoliina/Huhtinen, Aki-Mauri (2023). **Fehlinformation und Desinformation in Sozialen Medien als Impuls für die finnische nationale Sicherheit**. In: Eva Moehlecke de Baseggio/Olivia Schneider/Tibor Szvrircsev Tresch (Hg.). Soziale Medien und die Streitkräfte, 257–281.

Omand, David (2017). **Social Media Intelligence (SOCMINT)**. In: Robert Dover/Huw Dylan/Michael S. Goodman (Hg.). The Palgrave handbook of security, risk and intelligence. London, Palgrave Macmillan, 355–371.

Pawelec, Maria/Sievi, Luzia (2023). **Falschinformationen in den sozialen Medien als Herausforderung für deutsche Sicherheitsbehörden und -organisationen**. KrimOJ 5 (4). https://doi.org/10.18716/ojs/krimoj/2023.4.7.

Pennycook, Gordon/Rand, David G. (2022). **Nudging Social Media toward Accuracy**. The Annals of the American Academy of Political and Social Science 700 (1), 152–164. https://doi.org/10.1177/00027162221092342.

Pohle, Julia/Thiel, Thorsten (2019). **Digitale Vernetzung und Souveränität: Genealogie eines Spannungsverhältnisses**. In: Isabelle Borucki/Wolf Jürgen Schünemann (Hg.). Internet und Staat. Perspektiven auf eine komplizierte Beziehung. Baden-Baden, 57–80.

Prier, Jarred (2017). **Commanding the Trend: Social Media as Information Warfare**. Strategic Studies Quarterly (Winter), 50–85.

Pykett, Jessica/Jones, Rhys/Whitehead, Mark/Huxley, Margo/Strauss, Kendra/Gill, Nick/McGeevor, Kate/Thompson, Lee/Newman, Janet (2011). **Interventions in the political geography of 'libertarian paternalism'**. Political Geography 30 (6), 301–310. https://doi.org/10.1016/j.polgeo.2011.05.003.

Reuter, Christian/Kaufhold, Marc-André (2021). **Soziale Medien in Notfällen, Krisen und Katastrophen**. In: Christian Reuter (Hg.). Sicherheitskritische Mensch-Computer-Interaktion. Wiesbaden, Springer Fachmedien Wiesbaden, 407–430.

Roggenkamp, Jan Dirk (2019). **§ 21 Datenschutz und präventive Tätigkeit der Polizei**. In: Louisa Specht/Reto Mantz (Hg.). Handbuch Europäisches und deutsches Datenschutzrecht. Bereichsspezifischer Datenschutz in Privatwirtschaft und öffentlichem Sektor. München.

Roozenbeek, Jon/van der Linden, Sander (2019). **Fake news game confers psychological resistance against online misinformation**. Palgrave Communications 5 (1). https://doi.org/10.1057/s41599-019-0279-9.

Roozenbeek, Jon/van der Linden, Sander/Goldberg, Beth/Rathje, Steve/Lewandowsky, Stephan (2022). **Psychological inoculation improves resilience against misinformation on social media**. Science advances 8 (34), eabo6254. https://doi.org/10.1126/sciadv.abo6254.

Rostalski, Frauke (2024). **Die vulnerable Gesellschaft. Die neue Verletzlichkeit als Herausforderung der Freiheit**. C.H.Beck München.

Scherndl, Gabriele (2024). **Nein, Schleswig-Holstein hat die Rechtschreibung nicht abgeschafft**. Correctiv vom 28.05.2024. Online verfügbar unter https://correctiv.org/faktencheck/2024/05/28/nein-schleswig-holstein-hat-die-rechtschreibung-nicht-abgeschafft/ (abgerufen am 10.02.2025).

Schlömer, Jan/Kehrberg, Stefan (2025). **Demokratien unter Druck: Wie Desinformation Wahlen beeinflusst**. Zeitschrift für Rechtspolitik, 2–6.

Schnellenbach, Jan (2012). **Nudges and norms: On the political economy of soft paternalism**. European Journal of Political Economy 28 (2), 266–277. https://doi.org/10.1016/j.ejpoleco.2011.12.001.

Schoch, Friedrich (2011). **Die Schwierigkeiten des BVerfG mit der Bewältigung staatlichen Informationshandelns**. Neue Zeitschrift für Verwaltungsrecht, 193–198.

Schwarz, Kyrill-A. (2017). **Meinungsfreiheit und Persönlichkeitsschutz**. Juristische Arbeitsblätter, 241–244.

Sellnow, Timothy L./Seeger, Matthew W. (2013). **Theorizing Crisis Communication**. s.l., Wiley-Blackwell.

Sevignani, Sebastian (2017). **Krise der Privatheit. Zur Dialektik von Privatheit und Überwachung im informationellen Kapitalismus**. In: Kornelia Hahn/Andreas Langenohl (Hg.). Kritische Öffentlichkeiten - Öffentlichkeiten in der Kritik. Wiesbaden, 237–254.

SieberAdvisors GmbH (Hrsg.) (2025). **Renaissance der Rede. Fünf Erkenntnisse zur Krisenkommunikation der Münchner Polizei**. Online verfügbar unter https://sieber-advisors.de/krisenkommunikation-der-muenchner-polizei/ (abgerufen am 07.02.2025).

Sievi, Luzia/Pawelec, Maria (2025). **(How) Should security authorities counter false information on social media in crises? A democracy-theoretical and ethical reflection**. International Journal of Disaster Risk Reduction 116. https://doi.org/10.1016/j.ijdrr.2024.105093.

Stieglitz, Stefan/Brachten, Florian/Ross, Björn/Jung, Anna-Katharina (2017). **Do Social Bots Dream of Electric Sheep? A Categorisation of Social Media Bot Accounts**. Australasian Conference on Information Systems, 1–11.

Stroud, Scott R. (2019). **Pragmatist Media Ethics and the Challenges of Fake News**. Journal of Media Ethics 34 (4), 178–192. https://doi.org/10.1080/23736992.2019.1672554.

Struzina, Victor/Heller, Felix (2025). **Zur verwaltungsrechtlichen Einordnung von "Trusted Flaggern"**. Neue Zeitschrift für Verwaltungsrecht, 23–28.

Technisches Hilfswerk: **Virtual Operations Support Team (VOST)**. Online verfügbar unter https://www.thw.de/SharedDocs/Einheiten/DE/006_vost.html, zuletzt geprüft am 23.04.2025.

Thieltges, Andree/Hegelich, Simon (2017). **Manipulation in sozialen Netzwerken. Risikopotenziale und Risikoeinschätzungen**. Zeitschrift für Politik 64 (4), 493–512.

Ueberschär, Ellen (2021). **2.1.1 Freiheit. Grundrechte im digitalen Zeitalter und wie sie garantiert werden können**. In: Chris Piallat (Hg.). Der Wert der Digitalisierung. Gemeinwohl in der digitalen Welt, 101–122.

Veil, Shari R./Buehner, Tara/Palenchar, Michael J. (2011). **A Work-In-Process Literature Review: Incorporating Social Media in Risk and Crisis Communication**. Journal of Contingencies and Crisis Management 19 (2), 110–122. https://doi.org/10.1111/j.1468-5973.2011.00639.x.

Venzke-Caprarese, Sven (2013). **Social Media Monitoring. Analyse und Profiling ohne klare Grenzen?** Datenschutz und Datensicherheit 12, 775–779.

Vese, Donato (2022). **Governing Fake News: The Regulation of Social Media and the Right to Freedom of Expression in the Era of Emergency**. European Journal of Risk Regulation 13 (3), 477–513. https://doi.org/10.1017/err.2021.48.

Wagner, Daniel/Görgen, Thomas (2018). **Polizeiliche Kriminalprävention via Social media**. In: Axel Dessecker/Martin Rettenberger (Hg.). Medien - Kriminalität - Kriminalpolitik. Wiesbaden, Eigenverlag Kriminologische Zentralstelle, 53–82.

Waidner, Michael/Steinebach, Martin/Kreutzer, Michael (2020). **Technische Erkennung von Desinformation. Von Kopien über Montagen bis zu Deep-Fake-Videos**. In: Anja Hentschel/Gerrit Hornung/Silke Jandt (Hg.). Mensch - Technik - Umwelt: Verantwortung für eine sozialverträgliche Zukunft. Festschrift für Alexander Roßnagel zum 70. Geburtstag. Baden-Baden, 199–208.

Walsh, James P./O'Connor, Christopher (2019). **Social media and policing: A review of recent research**. Sociology Compass 13 (1). https://doi.org/10.1111/soc4.12648.

Walther, Susanne (2007). **Subjektiv-öffentliche Rechte auf Erstattung von Strafanzeige und Durchführung strafrechtlicher Ermittlungen**. In: Heinz Müller-Dietz/Egon Müller/Karl-Ludwig Kunz et al. (Hg.). Festschrift für Heike Jung zum 65. Geburtstag am 23.04.2007. Baden-Baden, 1045–1060.

Warg, Gunter (2018). **Meinungsfreiheit zwischen Zensur und Selbstzensur**. DÖV - Die Öffentliche Verwaltung (1), 473–482.

Wegner, Maren/Wagner, Daniel/vom Feld, Lara/Struck, Jens (2020). **Die Polizei als ‚Influencerin'? – Zum Einfluss der Polizei auf sicherheitspolitische Diskurse: Die Silvesternacht in Leipzig-Connewitz 2019/2020**. In: Daniela Hunold/Andreas Ruch (Hg.). Polizeiarbeit zwischen Praxishandeln und Rechtsordnung. Empirische Polizeiforschungen zur polizeipraktischen Ausgestaltung des Rechts. Wiesbaden/Heidelberg, Springer, 39–73.

Welty, Ute (2017). **Amoklauf in München vor einem Jahr: Wie die Polizei soziale Netzwerke nutzte. Marcus da Gloria Martins im Gespräch mit Ute Welty**. Deutschlandfunk Kultur vom 22.07.2017. Online verfügbar unter https://www.deutschlandfunkkultur.de/amoklauf-in-muenchen-vor-einem-jahr-wie-die-polizei-soziale-100.html (abgerufen am 15.08.2022).

Welzenbach-Vogel, Ines Clara (2021). **Gefilterte Ansichten. Zur Rolle von Filterblasen und Echokammern bei der Nutzung, Verarbeitung und Aneignung von Fake News und Verschwörungstheorien**. In: Michael Bauer/Laura Deinzer (Hg.). Zwischen Wahn und Wahrheit. Wie Verschwörungstheorien und Fake News die Gesellschaft spalten. Berlin, 185–209.

Foto: Margret Garbrecht

Maria Pawelec studierte Politik- und Verwaltungswissenschaft sowie Europawissenschaften in Konstanz, Istanbul, Bath und Berlin. Seit 2016 forscht sie am Internationalen Zentrum für Ethik in den Wissenschaften (IZEW) der Eberhard Karls Universität Tübingen u.a. zu den Themen Überwachung und Big Data, Informations- und Kommunikationstechnologien für Entwicklung, Technikgovernance, Technikfolgenabschätzung und zum Metaversum. Ein besonderer Forschungsschwerpunkt liegt auf Desinformation, Deepfakes und dem Einflüss künstlicher Intelligenz auf die Demokratie.

Michelle Duda studierte Rechtswissenschaft an der Universität zu Köln und der Università degli studi di Verona. Sie promoviert an der Universität zu Köln im Bereich der Cyberaggression. Ihre Forschung am Lehrstuhl für Strafrecht, Strafprozessrecht, Rechtsphilosophie und Rechtsvergleichung fokussiert die digitalen und internationalen Herausforderungen durch Desinformationen für das Individuum, die Gesellschaft und das Recht.

Foto: Lars Neumann

Dr. Luzia Sievi studierte Politikwissenschaft, Neuere und Neueste Geschichte und Wirtschaftspolitik an der Universität Freiburg und promovierte dort in Politischer Theorie. Ihre Forschung am Internationalen Zentrum für Ethik in den Wissenschaften (IZEW) der Eberhard Karls Universität Tübingen umfasst Demokratietheorien, Populismus, Desinformation und Nachhaltigkeit.

Rechtssicher und ethisch reflektiert auf Falschinformationen reagieren

Falschinformationen können die öffentliche Sicherheit erheblich gefährden, indem sie beispielsweise in Krisensituationen Panik auslösen und die Arbeit von Einsatzkräften erschweren, aber auch indirekter indem sie das Vertrauen in staatliche Institutionen untergraben. Behörden und Organisationen mit Sicherheitsaufgaben (BOS) haben eine besondere Verantwortung, gegen Falschinformationen vorzugehen, um die Sicherheit zu wahren, müssen aber gleichzeitig Grundrechte und demokratische Werte wie die Meinungsfreiheit achten. Diese Handreichung bietet BOS daher eine fundierte, ethisch und rechtlich reflektierte Orientierung im Umgang mit Falschinformationen in den sozialen Medien. Sie basiert auf der empirischen Forschung sowie der ethischen und rechtlichen Reflexion im interdisziplinären Projekt PREVENT (2022–2025), das vom Bundesministerium für Bildung und Forschung gefördert wurde.

Die Handreichung enthält rechtliche Grundlagen, unter anderem zu den Themen Datenschutz und behördliche Zuständigkeiten, sowie eine systematische Übersicht möglicher Gegenmaßnahmen. Diese Maßnahmen werden ethisch sowie rechtlich bewertet. Die Handreichung vermittelt sowohl theoretische Grundlagen als auch Anregungen zur praktischen Anwendung durch Reflexionsfragen, Quizze und praktische sowie juristische Fallbeispiele. Sie dient der Sensibilisierung, Aufklärung und Information von BOS-Mitarbeitenden sowie Ehrenamtlichen im Bereich der zivilen Sicherheit. Die Handreichung ermöglicht BOS eine verantwortungsvolle Auswahl und Umsetzung von Gegenmaßnahmen im Einklang mit demokratischen, ethischen und rechtsstaatlichen Prinzipien und leistet einen wichtigen Beitrag zur Bekämpfung sicherheitsgefährdender Falschinformationen in den sozialen Medien.

ISBN: 978-3-935933-23-0

EBERHARD KARLS UNIVERSITÄT TÜBINGEN

PREVENT

UNIVERSITÄT ZU KÖLN