

Desinformation in der Verwaltung: Falschinformationen bei der behördlichen Internetarbeit erkennen

Louis Jarvers mit Unterstützung von Sven Jovy und Jana Beyer

1. Einleitung: Desinformation ist eine gesamtgesellschaftliche Bedrohung und betrifft die Verwaltung als digitale Falschinformationen unmittelbar

In der Verwaltung und Behörden arbeiten Mitarbeitende mit Informationen aus dem Internet, deren Menge und Anzahl an Beteiligten rapide wächst. Veränderte oder komplett gefälschte Text-, Audio-, Bild- oder Videobeiträge mischen sich unter originales Material und beeinflussen die digitale Wahrnehmung. Staatlich-koordinierte und nicht-staatliche Einflusskampagnen generieren, verbreiten und verstärken Falschinformationen, unter anderem mit Hilfe künstlicher Intelligenz.

Bei behördlichen Kommunikationsprozessen wie Bürgerdiensten, Antragsverfahren oder öffentlichen Mitteilungen besteht die Gefahr, dass Desinformation Verwaltungsabläufe erheblich stören kann. Beispielsweise können manipulierte Informationen über Vorgänge, Verfahren oder Zuständigkeiten die Arbeit der Mitarbeitenden und das Vertrauen der Bürgerinnen und Bürger beeinträchtigen. Gerade bei komplexen Themen wie Gesundheit, Bildung oder Sozialleistungen werden tausende Nachrichten im Internet geteilt, so dass die Wahrscheinlichkeit steigt, dass Falschinformationen Entscheidungsprozesse und Kommunikationskanäle erreichen. Der Anspruch einer offenen, erreichbaren Verwaltung steht so im Konflikt mit einer digitalen Kommunikation, die Falschinformation enthält. Außerdem stellen Falschinformationen Verwaltungen vor Herausforderungen wie Vertrauensverlust, Ressourcenbindung bei der Bewertung und ggf. Bekämpfung, Risikoabwägung zur technologischen Dynamik, rechtliche Unsicherheiten, emotionale Beeinträchtigung bei Mitarbeitenden, Cybersicherheitsrisiken oder vertiefte Kommunikationsprobleme.

Dieses Papier beleuchtet das Phänomen Desinformation in der öffentlichen Verwaltung kurz und bietet eine Handreichung zur zeitkritischen Bewertung von Falschinformationen, insbesondere aus dem Internet, an.

Das <u>Bundesamt für Verfassungsschutz definiert Desinformation</u> als die absichtliche Verbreitung falscher oder irreführender Informationen. Diese bewusste Beeinflussung hat <u>laut Bundesministerium des Inneren</u> das Ziel, öffentlichen Meinungsbildung zu beeinflussen, eigenen Aktivitäten zu verschleiern, kontroversen Debatten zu emotionalisieren, gesellschaftlicher Spannungen zu verstärken und Misstrauen in staatliche Institutionen und Regierungshandeln zu schüren. Aufgrund der immer intensiveren Nutzung digitaler Angebote und Kommunikationsplattformen stellt Desinformation eine wachsende Bedrohung für offene Gesellschaften dar, die auch die Verwaltung als Rückgrat des Staates mittel- und unmittelbar betrifft.

Gegen Desinformation abzugrenzen ist die Misinformation, die das unabsichtliche Teilen von falschen Informationen umfasst. Ebenfalls keine Desinformation sind <u>Satire</u>, <u>Parodien oder klar erkenntliche politische Stellungnahmen</u>.

Desinformation	Nachweislich falsche oder irreführende Informationen, die mit dem Ziel des wirtschaftlichen Gewinns oder der vorsätzlichen Täuschung der Öffentlichkeit konzipiert, vorgelegt und verbreitet werden und öffentlichen Schaden anrichten können.
Misinformation	Unabsichtliches Verbreiten von Falschinformationen ohne Intention Schaden anzurichten

Tabelle 1: Unterscheidung von Desinformation und Misinformation

Stand: 10. Februar 2025 Seite 1 von 5



Falschinformationen sind im behördlichen Kontext relevant, egal ob sie in den Bereich der Desinformation oder Misinformation fallen. Ihrer Verifikation und Bewertung kommen daher eine besondere Rolle zu – gerade, wenn es sich um Desinformation handelt, da somit der gezielten Verbreitung Einhalt geboten werden kann.

2. Verifikation: Training von Falschinformationserkennung für den Behördenkontext, insbesondere für Internet-Informationen

In Verwaltungsbehörden kann die Verifikation von Informationen in verschiedenen Kontexten notwendig sein: Die Überprüfung von Online-Bürgermeldungen, die Validierung von Antragsunterlagen, die Bewertung von Informationen in Krisenkommunikationsszenarien oder die Prüfung von Social-Media-Hinweisen bei behördlichen Angelegenheiten. Bei Routineaufgaben, wie der Bearbeitung von Anträgen oder der Überprüfung von Dokumenten, steht meist mehr Zeit für eine sorgfältige Prüfung zur Verfügung. In dringlichen Situationen müssen Mitarbeitende hingegen schnell die Authentizität und Relevanz von Informationen einschätzen.

Um beiden Anwendungsfällen – der gründlichen Recherche und der schnellen Einschätzung – gerecht zu werden, ist es ratsam, einen standardisierten Ablaufplan für Informationsverifikation zu entwickeln. Dieser sollte flexibel genug sein, um sowohl in Routinesituationen als auch in zeitkritischen Lagen angewendet zu werden.

Die folgende Checkliste bietet hierfür eine Hilfestellung. Sie basiert, unter anderem, auf dem "Verification Handbook" von Craig Silverman, dem "Trust Checking Prinzip" von codetekt und den Leitlinien von Bellingcat und wurde auf den behördlichen Bedarf angepasst. Sie konzentriert sich vor allem auf Überprüfungen im Rahmen von Meldungen im Internet (z.B. in Form von Social-Media-Beiträgen). Die vorliegende Liste ist ein Entwurfsstand, der im Rahmen der konkreten Anwendung angepasst und weiterentwickelt werden soll.

3. Quick-Check: Verifikation von Falschinformation mithilfe der 5W-Methode

Der Quick-Check mithilfe der 5W-Methode ermöglicht eine erste, grobe Überprüfung einer Information. Der Fokus liegt auf einem möglichst geringen Zeitaufwand, da in der Regel weniger als 2-3 Minuten für eine Überprüfung zur Verfügung stehen. Idealerweise erfolgt die Verifikation arbeitsteilig, sodass ausreichend Zeit für eine Bewertung und ggf. Identifizierung von Falschinformationen möglich ist.

W1: Wer teilt die Information?

Um die Vertrauenswürdigkeit einer Information zu überprüfen, sollte prioritär geklärt werden, wer die Information teilt, ob die Quelle bereits bekannt ist und ob diese als verlässlich eingestuft werden kann. Dabei ist es hilfreich, frühere Informationen aus dem Profil zu betrachten, um die bisherige Zuverlässigkeit der Quelle zu prüfen. Möglicherweise lassen sich so bereits unauthentische Accounts oder "Internet-Trolle" identifizieren. Sie können Hinweise darauf geben, ob die Information authentisch ist oder Falschinformation mit einer Intention verbreitet werden.

- Ist der Verfasser/die Verfasserin des Beitrags bekannt?
- Ist das Profil des Verfassers vertrauenswürdig?
- Kann ein Fake- oder Troll-Account ausgeschlossen werden?
- Ist der Beitrag eine Primärquelle? Falls nicht, ist die Primärquelle bekannt?

Stand: 10. Februar 2025 Seite 2 von 5



W2: Was ist der Inhalt der Information?

Dem Inhalt der Information gilt grundsätzlich eine kritische Haltung. Naturgemäß ist die Sichtweise von Bürger:innen subjektiv und muss eingeordnet werden. Die Informationen sollten mit möglichen weiteren Informationen vom Ort, Vorgangshistorie oder Informationen anderer Quellen abgeglichen werden. Die Information, unerheblich in welcher Form, sollte in jedem Fall rückwärts geprüft werden. Falls im Rahmen eines Social-Media-Beitrags ein Foto oder vorliegender Textbausteine bereits häufiger in Verwendung waren, deutet es auf Trittbrettfahrer oder manipulative Absichten hin.

- Ist der Inhalt überprüfbar?
- Ist der Inhalt von anderen unabhängigen Quellen bestätigt?
- Passt die Information in den Kontext?
- Ist der Inhalt in anderen Kontexten geteilt worden? (Rückwärtssuche hilfreich)

W3: Wann wurde die Information geteilt?

Um die Aktualität und damit Relevanz einer Information zu bewerten, ist es wichtig zu wissen, wann sie geteilt wurde. Dabei sollte sichergestellt werden, dass die Primärquelle der Information vorliegt. Hier besteht stets die Möglichkeit, dass zwar relevante Orte identisch sind, Bilder, Videos oder sonstige Informationen jedoch von einem anderen (früheren) Zeitpunkt stammen. Hierfür bietet sich auch eine Rückwärtssuche der Inhalte an.

- Ist ein Datum aus Inhalt oder Kontext des Posts eingrenzbar?
- Ist die Information zeitlich relevant?
- Sind Metadaten oder andere Beiträge verfügbar, die das Datum bestätigen?
- Ist der Inhalt bereits früher verbreitet worden? (Rückwärtssuche hilfreich)

W4: Wo wurde der Beitrag abgesetzt?

Um die Unabhängigkeit der Quelle zu prüfen, sollte ermittelt werden, wo der Beitrag abgesetzt wurde. Es gilt zum Beispiel zu klären, ob der Verfasser tatsächlich in der Nähe eines beschriebenen Ortes ist und damit neue Erkenntnisse liefert oder Informationen nur weitergibt. Bei digitalen Informationen helfen möglicherweise Metadaten der Dateien oder Social-Media-Beiträge und Kommentare anderer Nutzer, die Aktualität und den Ort der Information zu bestätigen. Falls sich die Quelle tatsächlich vor Ort befindet, muss darüber hinaus geprüft werden, ob sich diese in Gefahr befindet und im Idealfall auch die Identität der Quelle geklärt werden.

- Ist ein Ort aus Inhalt oder Kontext der Information eingrenzbar?
- Passt dieser Ort zum Verfasser? Ist die Kenntnis möglich/logisch?
- Ist der Ort plausibel? (z. B. Nähe des Urhebers zum beschriebenen Ort)
- Sind Metadaten oder andere Informationen verfügbar, die den Ort bestätigen?

W5: Warum wurde der Beitrag abgesetzt?

Der Blick auf die mögliche Intention des Verfassers hilft, die Authentizität zu bewerten. Wenn offensichtliche Ziele einer digitalen Information, wie Werbung, Clickbaiting oder offensichtliche Selbstdarstellung, im Vordergrund stehen, ist es möglich, dass Inhalte übertrieben dargestellt werden oder die vorliegende Information nicht die Primärquelle ist. Reißerische Überschriften und Kommentare können auf das absichtliche Verbreiten der Informationen mit der möglichen Absicht der Stimmungsmache hindeuten. Eine bewusste Emotionalisierung der Situation kann für die Bewertung von, gerade zeitkritischen, Vorgängen wichtig sein.

Stand: 10. Februar 2025 Seite 3 von 5



- Ist eine klare Intention des Verfassers offensichtlich? Welche Konsequenz hat dies für die Authentizität der Information?
- Handelt es sich um Clickbaiting oder Werbung?
- Können Stimmungsmache oder Schadabsicht ausgeschlossen werden?
- Können Trittbrettfahrer oder Nachahmer ausgeschlossen werden?

Fazit: Eine Checkliste ersetzt weder Bauchgefühl noch Teamwork

Die Prüfschritte entlang der 5W-Methode bieten Anhaltspunkte, um Falschinformation zu erkennen und die Glaubwürdigkeit von Internet-Informationen unter Zeitdruck zu bewerten. Die Schritte können hierfür bei allen Online-Informationen, wie Social-Media-Beiträgen, Bildern, Videos, Dateien oder Webseiten angewandt werden. Auch für "Offline-Information" können hiermit bewertet werden, wenngleich nicht alle Schritte genau passen und ggf. angepasst werden müssen.

Für eine tiefgreifende Verifizierung können die Ansätze des Deep-Dive genutzt werden; diese finden sich in einer ausführlichen Fassung im Anhang 2 dieses Dokuments. Für diese Vertiefung sind zum Teil technische Fähigkeiten und grundsätzlich deutlich mehr Zeit nötig. Nichtsdestotrotz kann eine Information über weiterführende Verifikationsmöglichkeiten auch dann informativ und hilfreich sein, wenn in der Regel "nur" nach der 5W-Methode gearbeitet wird. Für eine weitere Professionalisierung der Verifikation bei der behördlichen Internet-Arbeit ist es zudem unerlässlich, dass die Bewertung von möglichen Falschinformationen nicht durch eine Person alleine vorgenommen wird. Das Vier- oder Mehraugenprinzip, sowie der Austausch im Team können wesentliche Hilfe bei der Verifikation leisten und besonders bei zeitkritischen Recherchen Fehler vermeiden.

Bei allen Empfehlungen, Methoden oder Checklisten ist abschließend wichtig, dass praktische Erfahrung und eigene Intuition im Internet ein hilfreiches Mittel sein können. Wenngleich die menschliche Bewertung immer kognitiven Verzerrungen (sog. Biases) unterliegt, sollte "das Bauchgefühl" unbedingt als Warnsignal ernst genommen werden – gerade dann, wenn sich nicht unmittelbar Ansatzpunkte entlang standardisierter Checklisten finden lassen. Auch in diesem Fall ist eine Rückfrage mit Kollegen hilfreich, um zu vermeiden, dass Falschinformationen durch fehlende oder fehlerhafte Verifikation behördliche Entscheidungen beeinflussen.

Über die Autor:innen

Louis Jarvers ist Manager bei der PD mit Schwerpunkt öffentliche Sicherheit, neue Technologien und Open Source Intelligence (OSINT). Parallel forscht er als Doktorand am Forschungszentrum Informatik des Karlsruher Instituts für Technologie (KIT) zu Sicherheit in der digitalen Demokratie, insbesondere Desinformation, Polarisierung und Online-Plattformen. Zuvor hat er Public Administration (Verwaltungswissenschaft) und Data Science an der Columbia University in New York und der Hertie School in Berlin, sowie der Universität Witten/Herdecke studiert. Als Teil seiner Forschung und Mitglied der PD-Expert Group Öffentliche Sicherheit befasst er sich wissenschaftlich wie praktisch mit Fragen der digitalen Transformation von Demokratie und Sicherheit.

Sven Jovy beschäftigt sich im Rahmen der Forschungsvereinigung Resilienz gegen Desinformation e.V. mit dem staatlichen Umgang mit Desinformation und hybrider Kriegführung. Er hat Sozialwissenschaft an der Universität zu Köln und Politikwissenschaft mit dem Schwerpunkt Sicherheitspolitik an der RWTH Aachen studiert. Sven Jovy arbeitet als Intellligence-Officer auf einer Leitstelle der Polizei in NRW.

Stand: 10. Februar 2025 Seite 4 von 5



Anlagen

- Anhang 1: Kurzübersicht zum Quick-Check (Verifikation von Falschinformation mithilfe der 5W-Methode)
- Anhang 2: Deep Dive: Ansätze für eine vertiefte technische und fachliche Verifikation

Stand: 10. Februar 2025 Seite 5 von 5



Kurzübersicht zum Quick-Check: Verifikation von Falschinformation mithilfe der 5W-Methode

Anhang 1 | Der Quick-Check mithilfe der 5W-Methode ermöglicht eine erste, grobe Überprüfung einer Information mit weniger als 2-3 Minuten Zeitaufwand für eine Überprüfung.

W1: Wer teilt die Information?	
Im die Vertrauenswürdigkeit einer Information zu überprüfen, sollte prioritär geklärt werden, wer ie Information teilt, ob die Quelle bereits bekannt ist und ob diese seriös ist.	
☐ Ist der Verfasser des Beitrags bekannt?	
☐ Ist das Profil des Verfassers vertrauenswürdig?	
☐ Kann ein Fake- oder Troll-Account ausgeschlossen werden?	
☐ Ist der Beitrag eine Primärquelle? Falls nicht, ist die Primärquelle bekannt?	
W2: Was ist der Inhalt der Information?	
Dem Inhalt der Information gilt grundsätzlich eine kritische Haltung. Naturgemäß ist die Sichtweise von Verfassern subjektiv und muss eingeordnet werden. Ist der Inhalt überprüfbar?	
☐ Ist der Inhalt von anderen unabhängigen Quellen bestätigt?☐ Passt die Information in den Kontext?	
\square Ist der Inhalt in anderen Kontexten geteilt worden? (Rückwärtssuche hilfreich)	
W3: Wann wurde die Information geteilt?	
Um die Aktualität und damit Relevanz einer Information zu bewerten, ist es wichtig zu wissen, wann sie geteilt wurde. Dabei sollte sichergestellt werden, dass die Primärquelle der Information vorliegt.	
☐ Ist ein Datum aus Inhalt oder Kontext der Information eingrenzbar?	
☐ Ist die Information zeitlich relevant?	
☐ Sind Metadaten oder andere Beiträge verfügbar, die das Datum bestätigen?	
☐ Ist der Inhalt bereits früher verbreitet worden? (Rückwärtssuche hilfreich)	
W4: Wo wurde der Beitrag abgesetzt?	
Um die Unabhängigkeit der Quelle zu prüfen, sollte ermittelt werden, von wo der Beitrag abgesetzt wurde.	
☐ Ist ein Ort aus Inhalt oder Kontext des Posts eingrenzbar?	
☐ Passt dieser Ort zum Verfasser?	
\square Ist dieser Ort plausibel? (z. B. Nähe des Urhebers zum beschriebenen Ort)	
☐ Sind Metadaten oder andere Beiträge verfügbar, die den Ort bestätigen?	
W5: Warum wurde der Beitrag abgesetzt?	
Der Blick auf die mögliche Intention hilft, die Authentizität zu bewerten. Ist eine klare Intention des Urhebers offensichtlich? Welche Konsequenz hat dies für die Authentizität der Information	
☐ Handelt es sich um Clickbaiting oder Werbung?	
☐ Können Stimmungsmache oder Schadabsicht ausgeschlossen werden?	
☐ Können Trittbrettfahrer oder Nachahmer ausgeschlossen werden?	

Stand: 10. Dezember 2024 Anhang: Seite 1 von 6



Deep-Dive: Ansätze für eine vertiefte technische und fachliche Verifikation von Internet-Informationen

Anhang 2

A. Quelle und Seriosität

A.1 Grundlegende Quellenbewertung

Im Fokus steht zunächst, ob die Quelle der Information eine Einzelperson oder eine Organisation ist. Dabei spielt die Reputation der Quelle in der jeweiligen Branche eine entscheidende Rolle. Es ist wichtig, Informationen über den Autor zu finden, wie beispielsweise dessen Qualifikationen oder frühere Arbeiten. Diese Details können Hinweise auf die Zuverlässigkeit und Fachkompetenz der Quelle liefern.

A.2 Primär- und Sekundärguellen

Eine weitere wichtige Überprüfung ist, ob die Information auf eine Primärquelle zurückgeführt werden kann. Primärquellen bieten direkte und unverfälschte Daten, die für eine fundierte Analyse unerlässlich sind. Sekundärquellen oder eigene Informationen sollten herangezogen werden, um die Primärquelle zu bestätigen. Dies hilft, die Genauigkeit der Informationen zu gewährleisten.

A.3 Crossreferencing

Ein wesentlicher Schritt ist der Vergleich der Informationen mit anderen seriösen Nachrichtenquellen. Dabei sollte untersucht werden, ob dieselbe Geschichte auch von anderen bekannten und vertrauenswürdigen Medien berichtet wird. Crossreferencing bietet eine zusätzliche Ebene der Verifikation und hilft, die Glaubwürdigkeit der Informationen zu stärken.

A.4 Offizielle Statements

Die Suche nach offiziellen Statements oder Klarstellungen von Organisationen oder Personen, die in der Nachricht erwähnt werden, ist ebenfalls von Bedeutung. Viele Organisationen veröffentlichen Richtigstellungen oder zusätzliche Informationen auf ihren offiziellen Kanälen, was eine wertvolle Ressource für die Validierung von Informationen darstellt.

A.5 Überprüfung von Zitaten und Referenzen

Es ist notwendig, die im Beitrag genannten Zitate und Referenzen zu überprüfen. Dies beinhaltet die Bestätigung, dass die Quellen korrekt angegeben sind und nachverfolgt werden können. Eine genaue Überprüfung der Referenzen stellt sicher, dass die Informationen fundiert und vertrauenswürdig sind.

A.6 Domain-Überprüfung

Für Informationen von eigenständigen Webseiten ist die Überprüfung der Domain der Website wesentlich. Unseriöse Seiten nutzen oft ungewöhnliche Domain-Endungen oder absichtlich ähnlich aussehende Domains, um vertrauenswürdige Quellen zu imitieren (z.B. "news.com.co" anstatt "news.com"). Eine sorgfältige Überprüfung der Domain kann helfen, die Seriosität der Quelle zu beurteilen.

Stand: 10. Dezember 2024 Anhang: Seite 2 von 6



A.7 Impressum und Kontaktinformationen

Zuletzt ist die Überprüfung des Impressums und der Kontaktinformationen der Website wichtig. Seriöse Websites bieten normalerweise vollständige Informationen über die Verantwortlichen und die Redaktion. Ein klar gekennzeichnetes Impressum und transparente Kontaktinformationen sind Indikatoren für die Vertrauenswürdigkeit einer Quelle.

De	ep-Dive Checkliste A: Quelle und Seriosität
	Wer ist die Quelle der Information (Einzelperson, Organisation)?
	Welche Reputation hat die Quelle in der Branche?
	Gibt es Informationen über den Autor (z.B. Qualifikationen, frühere Arbeiten)?
	Kann die Information auf eine Primärquelle zurückgeführt werden?
	Können Sekundärquellen oder eigene Informationen die Quelle bestätigen?
	Vergleiche die Information mit anderen seriösen Nachrichtenquellen. Wird die gleiche Geschichte auch von anderen bekannten und vertrauenswürdigen Medien berichtet? (Crossreferencing)
	Suche nach offiziellen Statements oder Klarstellungen von Organisationen oder Personen, die in der Nach- richt erwähnt werden. Viele Organisationen veröffentlichen Richtigstellungen oder zusätzliche Informationen auf ihren offiziellen Kanälen.
	Vergleiche Zitate und Referenzen: Wurden die im Beitrag genannten Zitate und Referenzen geprüft? Sind die Quellen korrekt angegeben und kann man sie nachverfolgen?
	Achte auf die Domain der Website. Unseriöse Seiten nutzen oft ungewöhnliche Domain-Endungen oder absichtlich ähnlich aussehende Domains, um vertrauenswürdige Quellen zu imitieren (z.B. "news.com.co" anstatt "news.com").
	Überprüfe, ob die Website ein Impressum und klare Kontaktinformationen hat. Seriöse Websites bieten normalerweise vollständige Informationen über die Verantwortlichen und die Redaktion.
В. 2	Zeitpunkt und Erstveröffentlichung
Ein	wichtiger Aspekt bei der Bewertung von Informationen ist der Zeitpunkt der Erstveröffentlichung. Das genaue
	um und die Uhrzeit der Veröffentlichung geben Aufschluss darüber, wie aktuell die Informationen sind. Es ist entlich, die Aktualität der Information zu kennen, um ihre Relevanz und Genauigkeit im aktuellen Kontext

Es ist ebenso entscheidend zu prüfen, ob es seit der Erstveröffentlichung relevante Entwicklungen oder Korrekturen gegeben hat. Informationen können im Laufe der Zeit durch neue Erkenntnisse oder Ereignisse ergänzt oder korrigiert werden. Eine sorgfältige Überprüfung der neuesten Updates und Berichtigungen stellen sicher, dass die Informationen aktuell und korrekt bleiben.

Deep-Dive Checkliste B: Zeitpunkt und Erstveröffentlichung □ Wann wurde die Information erstveröffentlicht? □ Gab es seither relevante Entwicklungen oder Korrekturen?

einschätzen zu können.

Stand: 10. Dezember 2024 Anhang: Seite 3 von 6



C. Visuelle oder formelle Überprüfung

C.1 Echtheit von Bildern und Videos

Ein wesentlicher Schritt bei der Überprüfung von Informationen ist die Bestätigung der Echtheit von visuellen Medien wie Bildern und Videos. Hierbei sollte geprüft werden, ob diese Medien echt oder manipuliert sind. Tools wie die Reverse Image Search oder InVid und der Youtube Data Viewer können verwendet werden, um die Authentizität zu überprüfen. Diese Werkzeuge helfen dabei, festzustellen, ob die Bilder oder Videos bereits früher verwendet wurden oder aus ihrem ursprünglichen Kontext herausgerissen und in einem neuen Zusammenhang präsentiert wurden.

C.2 Überprüfung der Metadaten

Es ist ebenso wichtig zu prüfen, ob die Medien von der angegebenen Zeit und dem angegebenen Ort stammen. Eine Überprüfung der Metadaten, die oft in den digitalen Dateien eingebettet sind, kann Aufschluss darüber geben, wann und wo ein Bild oder Video aufgenommen wurde. Diese Metadaten helfen dabei, die Richtigkeit und den Kontext der visuellen Inhalte zu bestätigen. Dabei ist wichtig, dass Metadaten einfach verändert und somit gefälscht werden können. Sie dienen daher lediglich ein Indiz und sollten mit entsprechender Vorsicht bewertet werden.

C.3 Verwendung von Rückwärtssuche

Wenn visuelle Medien in einem Beitrag enthalten sind, sollte eine Rückwärtssuche mit Tools wie Google Reverse Image Search durchgeführt werden. Diese Methode ermöglicht es, zu überprüfen, ob das Bild echt ist und im richtigen Kontext verwendet wird. Durch die Identifikation der ursprünglichen Quelle und des Kontexts des Bildes kann die Genauigkeit der Darstellung im aktuellen Beitrag bewertet werden.

C.4 Formale Überprüfung

Zusätzlich zur visuellen Überprüfung sollten Beiträge auf formelle Fehler wie Rechtschreib- und Grammatikfehler überprüft werden. Unseriöse Beiträge enthalten häufig viele dieser Fehler, die bei professionellen Nachrichtenquellen selten vorkommen. Eine sorgfältige formale Überprüfung kann daher ein Indikator für die Seriosität und Professionalität der Quelle sein.

Deep-Dive Checkliste C: Visuelle oder formelle Überprüfung

Sind Bilder und Videos echt oder manipuliert (z.B. mittels Reverse Image Search überprüfen; Videos mittels
InVid oder Youtube Data Viewer ¹)? Wer die Bilder oder Videos im richtigen/originalen Kontext verwendet?
Stammen die Medien von der angegebenen Zeit und dem angegebenen Ort (Metadaten überprüfen)?
Finden sich im Beitrag Rechtschreib- und Grammatikfehler?

D. Inhaltliche Konsistenz und Kontext

D.1 Übereinstimmung mit bekannten Fakten und Ereignissen:

Ein entscheidender Faktor bei der Bewertung von Informationen ist die Übereinstimmung mit bekannten Fakten und Ereignissen. Es sollte überprüft werden, ob die dargestellten Informationen mit dem aktuellen Stand des

Stand: 10. Dezember 2024 Anhang: Seite 4 von 6

¹ https://citizenevidence.amnestyusa.org/



Wissens und historischen Ereignissen übereinstimmen. Abweichungen oder Widersprüche können auf Fehler oder Fehlinformationen hinweisen.

D.2 Überprüfung auf logische Fehler und Unstimmigkeiten:

Es ist ebenso wichtig, den Bericht auf logische Fehler oder Unstimmigkeiten zu überprüfen. Konsistenz in der Argumentation und Darstellung ist ein Indikator für die Zuverlässigkeit der Information. Logische Brüche oder nicht nachvollziehbare Schlussfolgerungen sollten kritisch hinterfragt werden.

D.3 Kontextanalyse

Der Kontext, in dem die Information präsentiert wird, spielt eine wesentliche Rolle. Dies umfasst die politische Lage, wirtschaftliche Bedingungen und andere relevante Umstände. Die neuen Informationen sollten sinnvoll in diesen bestehenden Kontext passen. Ein umfassendes Verständnis des Kontextes hilft dabei, die Bedeutung und Relevanz der Informationen richtig einzuschätzen.

D.4 Nutzung von Faktencheck-Websites

Faktencheck-Websites wie Mimikama.org, Snopes oder FactCheck.org können zur Verifizierung der Richtigkeit der Informationen herangezogen werden. Diese Plattformen bieten detaillierte Analysen und Berichte, die helfen können, die Genauigkeit der präsentierten Fakten zu bestätigen oder zu widerlegen. Sie können allerdings nur genutzt werden, wenn es sich nicht um sehr aktuelle Informationen handelt. Kein Eintrag auf einer Faktencheck-Seite ist daher keine Bestätigung der Echtheit!

D.5 Überprüfung wissenschaftlicher Studien

Wenn wissenschaftliche Studien zitiert werden, ist es notwendig zu überprüfen, ob diese in anerkannten, peer-reviewed Fachzeitschriften veröffentlicht wurden. Die Peer-Review ist ein Qualitätsmerkmal, das sicherstellt, dass die Forschung von anderen Experten begutachtet und bestätigt wurde. Darüber hinaus sollte geprüft werden, ob die Ergebnisse der Studien von anderen Fachleuten auf diesem Gebiet bestätigt wurden. Dies trägt zur Validität und Zuverlässigkeit der wissenschaftlichen Aussagen bei. Grundsätzlich kann auch durch eine einfache Suche der Fachzeitschrift überprüft werden, ob dieses aufgrund seiner wissenschaftlichen Standards in der Vergangenheit kritisiert wurde.

Deep-Dive Checkliste D: Inhaltliche Konsistenz und Kontext

Stimmt die Information mit bekannten Fakten und Ereignissen überein?
Gibt es logische Fehler oder Unstimmigkeiten im Bericht?
Was ist der Kontext der Information (z.B. politische Lage, wirtschaftliche Bedingungen)?
Wie passen die neuen Informationen in den bestehenden Kontext?
Sind Aussagen oder Teile von Aussagen auf Faktencheck-Websites wie Mimikama.org, Snopes, FactCheck.org überprüft worden?
Wenn wissenschaftliche Studien zitiert werden: Handelt es sich bei der Studie bzw. der Fachzeitschrift um ein anerkanntes, peer-reviewtes Magazin? Gibt es Kritik an den wissenschaftlichen Standards des Magazins?

Stand: 10. Dezember 2024 Anhang: Seite 5 von 6



E. Überprüfung auf Bias und Manipulation:

E.1 Anzeichen für voreingenommene Berichterstattung

Es ist wichtig, nach Anzeichen für eine voreingenommene Berichterstattung zu suchen. Dies kann sich in einer einseitigen Darstellung oder einer Verzerrung der Fakten zeigen. Eine kritische Analyse der Quelle und ihres Inhalts kann Hinweise darauf geben, ob eine bestimmte Agenda verfolgt wird. Dabei ist eine politische Positionierung oder Agenda nicht per se problematisch, sollte aber die Wachsamkeit bei der Bewertung erhöhen.

E.2 Überprüfung auf inhaltliche Informationsmanipulation

Ein weiterer wichtiger Aspekt ist die Überprüfung, ob die Information möglicherweise manipuliert wurde oder Teil einer Einflusskampagne ist. Dies erfordert eine Analyse des Inhalts auf mögliche Manipulation. Hinweise auf inhaltliche Informationsmanipulation finden sich hinsichtlich der Struktur (z. B. Differenz zwischen Überschrift und Textkörper, Inhaltliche Wiederholungen oder "leere Sätze", Informationsüberfrachtung, fehlender Quellen), der Emotion (z. B. emotionalisierende Sprache, Verschiebung der Ebenen von Sachlich zu Persönlich oder vice versa, Ich-orientierte Aussagen in vermeintlich wissenschaftlichen Artikeln) oder der Ausdrucksweise (z. B. viel Umgangs-/Vulgärsprache, vage Ausdrucksweise, viele Ich-/Du-Botschaften). Es ist ratsam, auf übertriebene oder stark emotionale Sprache zu achten. Falschinformationen nutzen oft reißerische Formulierungen, um starke Reaktionen hervorzurufen. Eine kritische Analyse der Sprache und des Tonfalls kann Hinweise darauf geben, ob die Information objektiv und sachlich präsentiert wird oder ob versucht wird, eine bestimmte emotionale Reaktion zu erzeugen.

E.3 Überprüfung auf Manipulation durch unnatürliche Verbreitung oder Verstärkung

Zusätzlich zur inhaltlichen Informationsmanipulation können Informationen auch durch unnatürliche Verbreitung oder Verstärkung manipuliert werden. Zusätzlich zur künstlichen Generierung können hier Hinweise auf gefälschte Accounts oder unverhältnismäßig starke "Gefällt mir", "Teilen" oder "Kommentierung" auffallen. Außerdem können gleiche Kommunikationsmuster (z. B. Nutzung gleicher Hashtags-Kombinationen) oder Hashtag-Spamming (massenhafte Verwendung von Hashtags in einem falschen Kontext) Aufschluss über eine unnatürliche Verstärkung geben.

Deep-Dive Checkliste E: Überprüfung auf Bias und Manipulation

Gibt es Anzeichen für eine voreingenommene Berichterstattung?
Wurde der Beitrag inhaltlich manipuliert (Struktur, Emotion, Ausdrucksweise)?
Wurde der Beitrag durch unnatürliche Verbreitung oder Verstärkung manipuliert?
Achte auf übertriebene oder stark emotionale Sprache. Falschinformationen nutzen oft reißerische Formu-
lierungen, um starke Reaktionen hervorzurufen.

Stand: 10. Dezember 2024 Anhang: Seite 6 von 6