Kompetenzzentrum
Öffentliche IT

KOMPETENZZENTRUM ÖFFENTLICHE INFORMATIONSTECHNOLOGIE

DIGITALE GLAUBWÜRDIGKEIT

Petra Hoepner

IMPRESSUM

Autoren:
Petra Hoepner

Gestaltung:
Reiko Kammer

Fotos:
André Wirsig

Mit freundlicher Unterstützung:

http://luegenmuseum.de/wb/

Herausgeber:
Kompetenzzentrum Öffentliche IT
Fraunhofer-Institut für Offene Kommunikationssysteme FOKUS
Kaiserin-Augusta-Allee 31, 10589 Berlin
Telefon: +49-30-3463-7173
Telefax: +49-30-3463-99-7173
info@oeffentliche-it.de
www.oeffentliche-it.de
www.fokus.fraunhofer.de

ISBN: 978-3-9818892-1-5

1. Auflage Oktober 2017

VORWORT

Eine Bankfiliale vor Ort, ein Mensch in Uniform, eine Urkunde, eine Dokumentarsendung oder eine Bewertung durch ein renommiertes Institut – all das ist für uns (meist) glaubwürdig.

Im Digitalen ist die Glaubwürdigkeit oft schwieriger zu beurteilen: Misstrauen, Unsicherheit und Vorsicht auf der einen Seite oder Sorglosigkeit und Gutgläubigkeit auf der anderen Seite prägen den alltäglichen Umgang. Dieser Zwiespalt wird besonders anhand der Medien deutlich. Als glaubwürdige Medien gelten nach einer Umfrage[1] das öffentlich-rechtliche Fernsehen bzw. Radio (71 bzw. 77 Prozent) sowie die Tageszeitungen (65 Prozent), im Gegensatz zum Internet (30 Prozent) und den Boulevardmedien (7 Prozent). Ähnliche Ergebnisse liefert eine Umfrage der EU-Kommission[2]. Soziale Medien halten weniger als ein Drittel (32 Prozent) für zuverlässig, werden in diesen doch Informationen schnell verbreitet, ohne sie zu prüfen. Politische Schlagwörter wie Fake News und Lügenpresse kennzeichnen den Wandel und die Unsicherheit, was glaubwürdig ist oder nicht.

Glaubwürdigkeit ist vielschichtig, aber fragil. Sie kann nicht durch einzelne Maßnahmen erreicht, jedoch durch ein einziges Ereignis zerstört werden.

Wie also kann Glaubwürdigkeit im Digitalen entstehen? Welchen Einfluss haben die verschiedenen Bestandteile der digitalen Umgebung? Welche Methoden und Techniken unterstützen Glaubwürdigkeit? Und wie kann man sie stärken?

Mit diesem Whitepaper möchten wir die verschiedenen Aspekte digitaler Glaubwürdigkeit beleuchten.

Ihr Kompetenzzentrum Öffentliche IT

---

[1] Infratest dimap, Umfrage bezüglich Glaubwürdigkeit der Medien, 2015, https://www.infratest-dimap.de/umfragen-analysen/bundesweit/umfragen/aktuell/glaubwuerdigkeit-der-medien/.

[2] EU Commission, Umfrage Medienpluralismus und Demokratie, 2016, http://ec.europa.eu/COMMFrontOffice/publicopinion/index.cfm/Survey/getSurveyDetail/instruments/SPECIAL/surveyKy/2119.

GLAUBWÜRDIGKEIT IST EINE SUBJEKTIVE EINSCHÄTZUNG, DIE VON VERSCHIEDENEN INDIVIDUELLEN PARAMETERN ABHÄNGT.

INHALTSVERZEICHNIS

1. THESEN

Glaubwürdigkeit ist eine wesentliche Voraussetzung für die digitale Transformation.
Digitale Wirtschaft und Zivilgesellschaft benötigen authentische, glaubwürdige Produkte, Märkte, Plattformen, Teilnehmer und Systeme für ihr Funktionieren. Unsicherheit und Zweifel behindern die digitale Transformation. Das Zusammenwirken von Menschen und Informationstechnik muss geeignet gestaltet werden, damit Glaubwürdigkeit und Vertrauen gestärkt und erhalten werden. Dabei können technische und organisatorische Mechanismen nur bedingt gesellschaftliche Probleme lösen, schlimmstenfalls verstärken sie diese sogar.

Fake ist nicht neu, erreicht online aber eine neue Dimension.
Fälschungen gab es schon immer. Durch veränderte Mediennutzung wird die Gesellschaft anfälliger dafür, Informationen falsch zu interpretieren oder gezielten Fälschungen zum Opfer zu fallen. Digitale Inhalte sind leicht zu erstellen, oft auch veränderbar und die Verbreitungswege für Informationen sind kostengünstig und vielfältig.

Digitale Glaubwürdigkeit beruht auf vielen Faktoren.
Ob im Digitalen Glaubwürdigkeit gegeben ist, hängt von der Glaubwürdigkeit diverser Vorgänge und Teilnehmer im Einzelnen und in ihrem Zusammenspiel ab, beispielsweise von Datenerhebung, Datenanalyse, Informations- und Wissensgenerierung und der Veröffentlichung auf Plattformen.

Glaubwürdigkeit ist kontextabhängig.
Glaubwürdigkeit ist eine subjektive Einschätzung, die von verschiedenen individuellen Parametern abhängt. Persönliche Erfahrungen, Bewertungen anderer oder Umgebungsparameter wie Ort, Zeit und Darstellung sind nur einige mögliche Einflussfaktoren. Technische Lösungen können in diesem Rahmen bloß eine Unterstützungsfunktion bieten, aber Glaubwürdigkeit weder beweisen noch erzwingen.

Glaubwürdigkeit und Sicherheit haben viele Gemeinsamkeiten.
100 Prozent glaubwürdig gibt es ebenso wenig wie 100 Prozent sicher. Trotz stärkender Maßnahmen bleibt ein Risiko, beispielsweise dass etwas manipuliert wurde. Scheint etwas relativ glaubwürdig oder sicher zu einem bestimmten Zeitpunkt, so kann sich diese Bewertung mit der Zeit verändern, da sich das Bewertungsobjekt oder die Umgebung ändern können. Die Mechanismen und Verfahren für Glaubwürdigkeit und Sicherheit sind oft ähnlich und unterliegen gleichermaßen einem Wettrüsten zwischen denen, die auf Glaubwürdigkeit beziehungsweise Sicherheit angewiesen sind, und den Angreifern oder Kriminellen, die Verwundbarkeiten für ihre Zwecke nutzen.

Anonymität und Pseudonymität stehen einer Glaubwürdigkeit nicht grundsätzlich entgegen.
Neben einer sicher identifizierten und authentisierten namentlichen Quelle gibt es weitere Anhaltspunkte, die zur Glaubwürdigkeitsabschätzung herangezogen werden können. Beispielsweise ist die Reputation ein wichtiges Kriterium.

Künstliche Intelligenz und autonome Systeme werfen neue Fragen auf.
Kann eine Maschine, ein Algorithmus oder ein autonomes System glaubwürdig sein? Alle sind abhängig von Daten. Lernende Systeme sind manipulierbar, wenn die Qualität der Daten nicht gewährleistet ist. Die Validität und Nicht-Manipulierbarkeit dieser Daten ist daher von immer größerer Bedeutung. Ebenso wichtig wie die Daten sind die Algorithmen, mit denen diese verarbeitet werden. Werte, Einstellungen und die Denkweise ihrer Autoren könnten sich auch im Algorithmus wiederfinden.

Nicht alle gesellschaftlichen Probleme können durch Technik gelöst werden.
Kommunikation erfüllt unterschiedliche Aufgaben, die Vermittlung eines Sachinhalts ist nur eine davon. Kommunikationsmittel werden für unerwünschte Zwecke missbraucht und Fake wird daher nie komplett unterbunden werden können. Folglich kann nur das Risiko auf ein gesellschaftlich verträgliches Minimum reduziert werden.

Aufbau der Ausstellung »unverbesserlich«, im großen Saal des Lügenmuseums im ehemaligen Gasthof Serkowitz, Radebeul

2. FAKE UND ANDERE HERAUSFORDERUNGEN

Fälschungen gab es schon immer. Ob Geld, Kunst, Nachrichten oder Ausweise – historisch gesehen wurde schon fast alles gefälscht. Die Gründe sind vielfältig. Manche fälschen aus wirtschaftlichen Gründen, anderen sind Macht, Ruhm, Ehre oder Aufmerksamkeit wichtig. Häufig ist auch die Grenze zu Straftaten nicht eindeutig. Das Spektrum variiert von betrügerischen Absichten, manipulativen Tendenzen, Imitation oder Täuschung bis hin zu Plagiaten und Produktpiraterie. Andererseits gibt es auch harmlose Fälschungen, besonders im künstlerischen Bereich wie Parodien, Satire oder Comedy.

Der englische Begriff »Fake« für Fälschung wird in letzter Zeit häufig verwendet und meist mit deren digitalen Ausprägungen in Verbindung gebracht.

Fake News sind gezielte Falschmeldungen im Internet, die Menschen täuschen sollen, um die öffentliche Meinungsbildung zu beeinflussen oder geschäftliche Interessen zu verfolgen.[3/4] Eine wesentliche Eigenschaft dieser Falschinformationen ist, dass sie nicht nachweisbar rückbestätigt werden können. Trotzdem finden diese Nachrichten eine weite Verbreitung, da sie von Lesern als wahr empfunden, manchmal sogar aufgrund der bloßen Überschrift weiterverbreitet werden. Von der Gesellschaft für Deutsche Sprache wurde »postfaktisch« zum »Wort des Jahres 2016« gewählt. Das Kunstwort verweist darauf, dass in politischen und gesellschaftlichen Diskussionen oftmals Emotionen anstelle von Fakten priorisiert werden.[5]

In anderen Konstellationen wird ebenfalls der Begriff Fake gebraucht. Fake Shops sind gefälschte Online-Shops, die die Angebote von realen Shops kopieren und für ihre kriminellen Zwecke nutzen. Fake Apps werden von Betrügern verbreitet, um das Geld oder die Daten der Kunden an sich zu bringen.[6] Beispiele sind Fake Shopping Apps für gefälschte Markenartikel oder Apps, die angeblich Freunde und Follower in sozialen Netzwerken generieren.

Eine weitere Form von Fake[7], Astroturfing, dient der Tarnung von Unternehmen oder Lobbyorganisationen, um die öffentliche Meinung zu beeinflussen oder auch um Produkte unterschwellig zu vermarkten.

Auch neue digitale Herausforderungen wie Filterblasen, die durch personalisierte, vorgefilterte Suchumgebungen eine auf den Aufrufer zugeschnittene Welt erzeugen, können manipulativ wirken und erschweren die objektive Abschätzung der digitalen Glaubwürdigkeit. Trolle[8] mischen sich in Online-Kommunikation ein, um zu provozieren oder Gerüchte und falsche Meldungen zu verbreiten. Cybermobber diffamieren ihre Mitmenschen und benutzen dafür häufig falsche Identitäten.

Unabhängig von den verschiedenen Intentionen der Fälschungen ist diesen gemeinsam, dass eigentlich Unglaubwürdiges oder Falsches glaubwürdig dargestellt wird. Das Digitale eröffnet hier eine neue Dimension:

- Die Reichweite von digitalen Aktivitäten ist überdimensional groß gegenüber den herkömmlichen Verbreitungsmöglichkeiten.
- Jeder kann Inhalte online veröffentlichen oder teilen und damit potenziell ein großes Publikum erreichen.
- Nutzer-generierte Inhalte sind von professionellen Inhalten nicht zu unterscheiden.
- Online-Informationen können (teilweise auch durch Unbefugte) jederzeit unbemerkt verändert werden.
- Die Identität von Personen ist im Internet leicht zu verschleiern.
- Unsere herkömmlichen Bewertungsmethoden für Glaubwürdigkeit funktionieren im Digitalen nur bedingt.

---

[3] Alexander Roßnagel u. a., Fake News, Policy Paper, Juni 2017, https://www.forum-privatheit.de/forum-privatheit-de/publikationen-und-downloads/veroeffentlichungen-des-forums.php.

[4] Kathrin Werner, Fake News – Wirkung oder Ursache des postfaktischen Zeitalters?, 20.12.2016, https://www.hdm-stuttgart.de/view_news?ident=news20161220172509.

[5] Matthias Heine, Was Sie über das »Wort des Jahres« wissen müssen, 9. 12. 2016, https://www.welt.de/kultur/article160136912/Was-Sie-ueber-das-Wort-des-Jahres-wissen-muessen.html.

[6] Benedikt Frank, So erkennen Sie betrügerische Fake-Apps, 12.3.2017, https://www.welt.de/wirtschaft/webwelt/article162785470/So-erkennen-Sie-betruegerische-Fake-Apps.html.

[7] Lobbypedia: Unter Astroturfing versteht man das künstliche Nachahmen einer Bürgerbewegung, die hinter den Kulissen von Unternehmen oder Lobbyorganisationen gesteuert oder finanziert wird. Die Tarnung soll den Geldgebern dazu dienen, von der besonderen Glaubwürdigkeit von Bürgerinitiativen zu profitieren. https://lobbypedia.de/wiki/Astroturfing.

[8] Duden: Troll – Internetnutzer, der die Teilnehmer einer Online-Community (z. B. eines Diskussionsforums, Chatrooms) durch regelwidriges, antisoziales Verhalten, besonders mit bestimmten (beleidigenden oder diskriminierenden) Kommentaren, gezielt provoziert, um eine entsprechende Reaktion hervorzurufen. http://www.duden.de/rechtschreibung/Troll_Noergler_Querulant.

3. FACETTEN VON GLAUBWÜRDIGKEIT

Täglich müssen wir Personen, Organisationen, Medien oder Informationen »Glauben schenken«, da eigenes Wissen oder eigene Erfahrungen nicht vorhanden sind. Wir schreiben dabei unserem Gegenüber Glaubwürdigkeit zu.

3.1. WAS IST EIGENTLICH GLAUBWÜRDIGKEIT?

Auch wenn es ein allgemeines Verständnis gibt, was Glaubwürdigkeit ist, so wird der Begriff in verschiedenen Fachgebieten unterschiedlich betrachtet.[9] Juristisch ist es etwa die Vertrauenswürdigkeit eines Zeugen, im Marketing die Glaubwürdigkeit von Produkten, Marken oder Werbeaussagen und in der Medienbranche die der Informationsquellen. Es mangelt an einer einheitlichen Definition. Den Kern der verschiedenen Definitionen könnte man folgendermaßen zusammenfassen:

GLAUBWÜRDIGKEIT IST DIE BEREITSCHAFT, ETWAS ALS RICHTIG UND WAHR ZU AKZEPTIEREN.[10]

Sinnverwandt beziehungsweise auch als Synonyme werden folgende Begriffe verwendet: Glaubhaftigkeit, Kredibilität, Plausibilität, Sicherheit, Verlässlichkeit, Zuverlässigkeit, Authentizität, Echtheit, Unabweisbarkeit, Unanfechtbarkeit, Unangreifbarkeit, Unbestreitbarkeit, Unwiderlegbarkeit, Wahrheit, Originalität, Aufrichtigkeit, Ehrlichkeit, Ernsthaftigkeit, Natürlichkeit, Seriosität, Vertrauenswürdigkeit, Redlichkeit.[11]

Analysiert man diese Begriffe, kann man feststellen, dass mehrere davon auch im Kontext Sicherheit und Vertrauen auftauchen. Das berechtigt zu der Annahme, dass Glaubwürdigkeit und Sicherheit sowie Vertrauen viele Gemeinsamkeiten haben. Jedoch ist keiner dieser Werte nur Ursache oder nur Wirkung des anderen, sondern sie bedingen sich gegenseitig.

Ist Glaubwürdigkeit eher vergangenheitsgerichtet, d. h., auf Grund bestimmter Aktivitäten wird Glaubwürdigkeit zugeschrieben, so ist Vertrauen eher zukunftsgerichtet und hat die Funktion zukünftige Unsicherheit zu reduzieren.[12]

Doch wie entsteht Glaubwürdigkeit? An welchen Indikatoren lässt sie sich messen? Welche technischen und organisatorischen Maßnahmen erzeugen und unterstützen Glaubwürdigkeit? Neben messbaren objektiven Einflüssen sind das oft weiche, subjektive Umstände. Es gibt Faktoren, die sich positiv auf die Glaubwürdigkeit auswirken, und Faktoren, die das Gegenteil tun.[13]

Glaubwürdigkeit ist ein multidimensionales Konstrukt. Am Beispiel Wikipedia lassen sich die verschiedenen Dimensionen von Glaubwürdigkeit verdeutlichen:[14]

- *Website:* Wikipedia selbst ist eine glaubwürdige Quelle.
- *Inhalt:* Ein spezifischer Eintrag bei Wikipedia ist glaubwürdig.
- *Autor(en):* Ein oder mehrere bestimmte Autoren sind glaubwürdig.

Gleichzeitig wirken die verschiedenen Dimensionen in komplexer Art und Weise zusammen, um Glaubwürdigkeit herzustellen, können aber ebenfalls im Konflikt stehen und die Beurteilung erschweren. Im Folgenden werden daher die unterstützenden oder reduzierenden Aspekte von Glaubwürdigkeit untersucht.

[9] Wikipedia Glaubwürdigkeit, https://de.wikipedia.org/wiki/Glaubw%C3%BCrdigkeit.

[10] Enzyklopädie der Werte: Definition Glaubwürdigkeit, https://www.wertesysteme.de/glaubw%C3%BCrdigkeit/.

[11] Ergebnis von Duden Synonymwörterbuch und http://www.synonyme-finden.com/.

[12] Waldemar Dzeyk, Vertrauen in Internetangebote, eine empirische Untersuchung zum Einfluss von Glaubwürdigkeitsindikatoren bei der Nutzung von Online-Therapie- und Online-Beratungsangeboten, Universität zu Köln 2005, http://kups.ub.uni-koeln.de/1606/.

[13] TeleTrusT (Hrsg.), Vertrauen und IT-Sicherheit, Vertrauensmodelle für die Informationsgesellschaft, TeleTrusT – Bundesverband IT-Sicherheit e. V. 2015, https://www.teletrust.de/publikationen/broschueren/vertrauensmodell/.

[14] Miriam J. Metzger / Andrew J. Flanagin, Credibility and trust of information in online environments, The use of cognitive heuristics, in: Journal of Pragmatics 59 (2013).

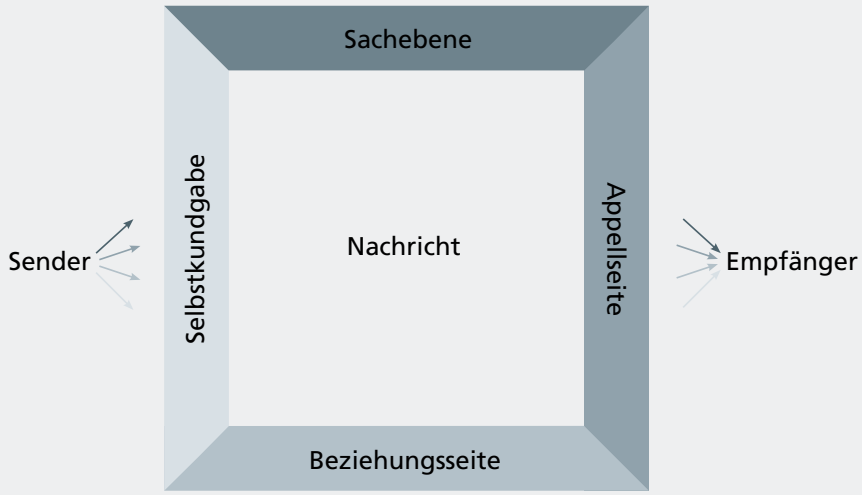

Abbildung 1: Vier-Seiten-Modell der Kommunikation nach Friedemann Schulz von Thun[16]

3.2. VIER-SEITEN-MODELL NACH FRIEDEMANN SCHULZ VON THUN

Die Kommunikationsforschung befasst sich mit menschlicher Kommunikation, ihren diversen Aspekten sowie möglichen Störfaktoren. Ein bekanntes Modell der Kommunikationspsychologie ist das »Vier-Seiten-Modell«[15] (auch Kommunikationsquadrat) von Friedemann Schulz von Thun. In diesem Modell (siehe Abbildung 1) werden übermittelte Nachrichten von verschiedenen »Seiten« (Aspekten, Ebenen) betrachtet: Sachinhalt, Selbstkundgabe, Beziehung und Appell.

Jede Nachricht kann nach Schulz von Thun mehrseitig gedeutet werden:

- *Sachebene:* worüber informiert die Nachricht (Fakten, Informationen, Inhalte etc.)
- *Selbstkundgabe:* was gibt der Sender / die Quelle von sich preis (Wünsche, Gefühle etc.)
- *Beziehungsseite:* was offenbart die Nachricht über die Beziehung zwischen Sender und Empfänger (Wert- oder Geringschätzung, Kritik etc.)
- *Appellseite:* was soll die Nachricht beim Empfänger veranlassen (Botschaft, Intention etc.)

Störungen der Kommunikation entstehen, wenn Sender und Empfänger die verschiedenen Ebenen unterschiedlich interpretieren.

Im Digitalen findet Kommunikation nicht direkt statt. Ein oder mehrere Intermediäre, Systeme oder Übertragungsmedien sind der Kommunikation von der Quelle zum Ziel zwischengeschaltet (beispielsweise wird das im Sender-Empfänger-Modell nach Shannon und Weaver[17] dargestellt, in dem Quelle und Sender sowie Empfänger und Ziel separat betrachtet werden). Störungen oder Verfälschungen können daher auch durch diese verursacht werden.

Es stellt sich die Frage, wie im Digitalen kommunikationspsychologisch Glaubwürdigkeit vermittelt werden kann, da technische Umgebungen ebenfalls multidimensional sind. In Anlehnung an das Vier-Seiten-Modell nach Schulz von Thun wird hier Glaubwürdigkeit als Vier-Seiten-Modell dargestellt: Die Appellseite dient im Wesentlichen dazu, die Intention der Quelle zu erfüllen, beispielsweise ein Produkt zu verkaufen, Informationen zu vermitteln oder Freunde zu gewinnen. Die Intention der Quelle liefert dabei einen wichtigen Anhaltspunkt zur Bewertung ihrer Glaubwürdigkeit. Um die Intention zu erreichen, wird auf der Sachebene ein Inhalt übermittelt, der Informationen, Dokumente oder Daten liefert. Da im Digitalen die Selbstkundgabe systembedingt unvollständig und schwer überprüfbar ist, ist man auf glaubwürdige digitale Identitäten angewiesen, um sich als Quelle authentisch darzustellen. Auf Beziehungsebene werden weitere subjektive Aussagen übermittelt, die hier als Medium (welche digitalen Medien oder Assets übermitteln diese Aussagen) und Kontext (wie stellt sich die digitale Umgebung dar) bezeichnet werden.

Abbildung 2 zeigt, dass sich auch im Digitalen die verschiedenen Dimensionen kommunikativer Handlungen als Seiten modellieren lassen, die sich gegenseitig beeinflussen und – in der kommunikativen Praxis – nicht eindeutig voneinander zu

[15] Kommunikationsquadrat (Vier-Seiten-Modell) nach Friedemann Schulz von Thun 1981, http://www.schulz-von-thun.de/modelle/kommunikationsquadrat.

[16] Wikipedia, Grafik Vier-Seiten-Modell, https://de.wikipedia.org/wiki/Vier-Seiten-Modell.

[17] Wikipedia, Sender-Empfänger-Modell, https://de.wikipedia.org/wiki/Sender-Empf%C3%A4nger-Modell.

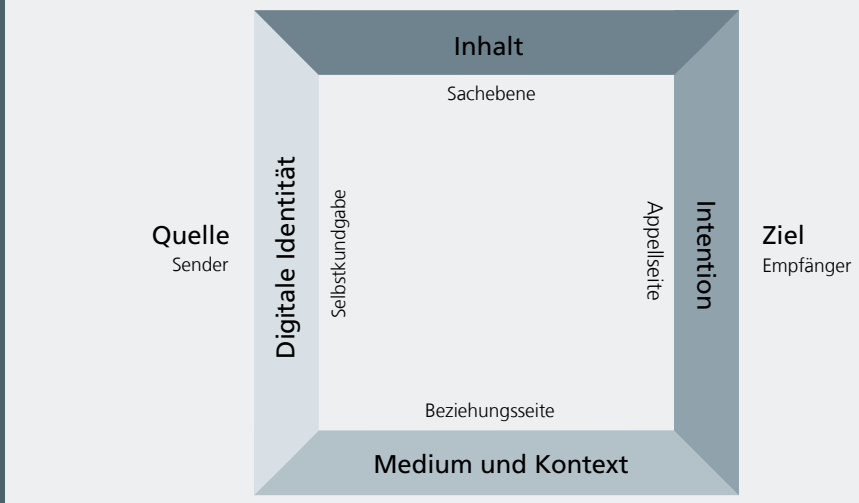

Abbildung 2: Vier-Seiten-Modell der digitalen Glaubwürdigkeit

trennen sind. Betrachtet man beispielsweise Falschinformationen, dann sinkt die Glaubwürdigkeit der Quelle, sobald man diese entdeckt. Hingegen können glaubwürdige Inhalte die Glaubwürdigkeit einer Quelle stärken, auch wenn man die Quelle nicht kennt. Im nächsten Abschnitt wird erläutert, wie Glaubwürdigkeit durch einen Empfänger eingeschätzt werden kann.

3.3 KOGNITIVE HEURISTIKEN

Um Glaubwürdigkeit zu beurteilen, geht jeder Empfänger von Informationen subjektiv vor. Dazu dienen sogenannte kognitive Heuristiken. Generell wird als Heuristik das Vorgehen bezeichnet, um trotz begrenzten Wissens oder unvollständiger Informationen und limitierter Zeit zu wahrscheinlichen Aussagen oder praktikablen Lösungen zu kommen.[18]

Verschiedene kognitive Heuristiken zur Evaluierung von Glaubwürdigkeit umfassen:[19/20]

- *Wiedererkennung:* Die Wiedererkennung des Namens von Quellen oder Websites fördert deren Glaubwürdigkeit, ohne dass intensivere Recherchen vom Empfänger durchgeführt werden müssen. Als psychologische Grundlage wird angenommen, dass Namenswiedererkennung mit positiven Transaktionen assoziiert wird.
- *Empfehlung:* Quellen werden als glaubwürdig eingeschätzt, wenn sie entweder von Bekannten empfohlen oder von Fremden durch Rezensionen oder Bewertungen als positiv eingeschätzt werden.
- *Konsistenz:* Informationen sind glaubwürdiger, wenn sie von verschiedenen Quellen übereinstimmend berichtet werden.
- *Selbstbestätigung:* Informationen werden als glaubwürdiger erachtet, wenn sie mit den eigenen Ansichten übereinstimmen, unabhängig davon, wie überzeugend sie recherchiert oder referenziert werden.
- *Verletzung der Erwartungshaltung:* Die Glaubwürdigkeit wird verringert, wenn Erwartungen nicht erfüllt werden, beispielsweise, wenn mehr Daten als erwartet erfragt werden, unstimmige Informationen bereitgestellt werden oder die Form der Darstellung hinsichtlich Rechtschreibung, Grammatik oder Navigation nicht professionell ist.
- *Überredungs-/Werbungsabsichten:* Negativ wirkt sich ebenfalls das Gefühl aus, manipuliert zu werden, beispielsweise durch Werbung oder andere versteckte Intentionen.

Die aufgeführten Heuristiken sind weder vollständig noch überschneidungsfrei. Sie dienen jedoch dazu, verschiedene Anhaltspunkte darzustellen, die die Glaubwürdigkeitsbewertung beeinflussen und schnelle (teilweise unbewusste) Denkprozesse einleiten.

[18] Wikipedia, Heuristik, https://de.wikipedia.org/wiki/Heuristik.

[19] Miriam J. Metzger / Andrew J. Flanagin / Ryan B. Medders, Social and Heuristic Approaches to Credibility Evaluation Online, in: Journal of Communication 60 (2010) 3.

[20] M. J. Metzger / A. J. Flanagin (Anm. 14).

Illumination des Lügenmuseums in Serkowitz von Claudia Reh zum Weltlügenball.

3.4 MODELL FÜR DIGITALE GLAUBWÜRDIGKEIT

Um die verschieden Facetten und die Komplexität digitaler Glaubwürdigkeit strukturiert darzustellen, wird aus dem Vier-Seiten-Modell nach Schulz von Thun (vgl. Abschnitt 3.2) und den kognitiven Heuristiken zur Beurteilung von Glaubwürdigkeit (vgl. Abschnitt 3.3) das Modell für digitale Glaubwürdigkeit abgeleitet und anschließend in Abbildung 3 dargestellt:

- *Empfänger:* Der Empfänger ist derjenige, der etwa aufgrund seines Vorwissens, seiner Erfahrungen oder seines Weltbildes Informationen (oder auch Dinge) als glaubwürdig einstuft.
- *Basis:* Verschiedene Quellen (Autoren, Organisationen oder auch Websites) übermitteln »Nachrichten« die der Empfänger für sich beurteilen muss. Für die Bewertung von Glaubwürdigkeit sind weitere Zusatzinformationen wichtig, etwa wie (Medium) und in welchem Bezugsrahmen (Kontext) eine Nachricht transportiert wird.
- *Anhaltspunkte:* Ob übermittelte Nachrichten glaubwürdig erscheinen, kann der Empfänger anhand verschiedenartiger Anhaltspunkte einschätzen. Diese differieren für verschiedene Dimensionen. Heuristiken ergänzen beziehungsweise kombinieren die unterschiedlichen Anhaltspunkte.
- *Technische Hilfsmittel:* Für die technische Umsetzung stehen diverse Hilfsmittel zur Verfügung. Diese werden im folgenden Modell für digitale Glaubwürdigkeit ungeordnet aufgelistet. Nicht jeder Anhaltspunkt korreliert mit einem spezifischen technischen Hilfsmittel. Technologien können nicht direkt Glaubwürdigkeit erzeugen, aus ihnen lassen sich jedoch objektivere Schlüsse ziehen, ob etwas als glaubwürdig eingeschätzt werden kann.

Ziel des Modells ist die Visualisierung der Komplexität von digitaler Glaubwürdigkeit auf einen Blick, ohne jedoch den Anspruch auf Vollständigkeit zu erheben. Im Modell werden verschiedene Anhaltspunkte oder Hilfsmittel auch mehrfach genannt, da sie unterschiedlich eingesetzt werden können.

Die folgenden Abschnitte erläutern bestimmte wichtige technische Hilfsmittel hinsichtlich ihrer Unterstützung von Glaubwürdigkeit näher. Begleitet werden die technischen Hilfsmittel durch strategische und organisatorische Maßnahmen, um Glaubwürdigkeit zu vermitteln. Einschränkend ist anzumerken, dass technische, strategische und organisatorische Maßnahmen nur dann Glaubwürdigkeit unterstützen oder stärken können, wenn diese im Wesentlichen mit Informationsvermittlung verbunden sind. Im Vier-Seiten-Modell nach Schulz von Thun entspricht das der Sachebene der Nachrichtenvermittlung. Nachrichten, die andere Ebenen der Kommunikation nutzen, um beispielsweise Gefühle zu vermitteln (Stärkung des Gemeinschaftsgefühls, Aufregung, teilweise auch Werbung), werden nicht im Modell erfasst.

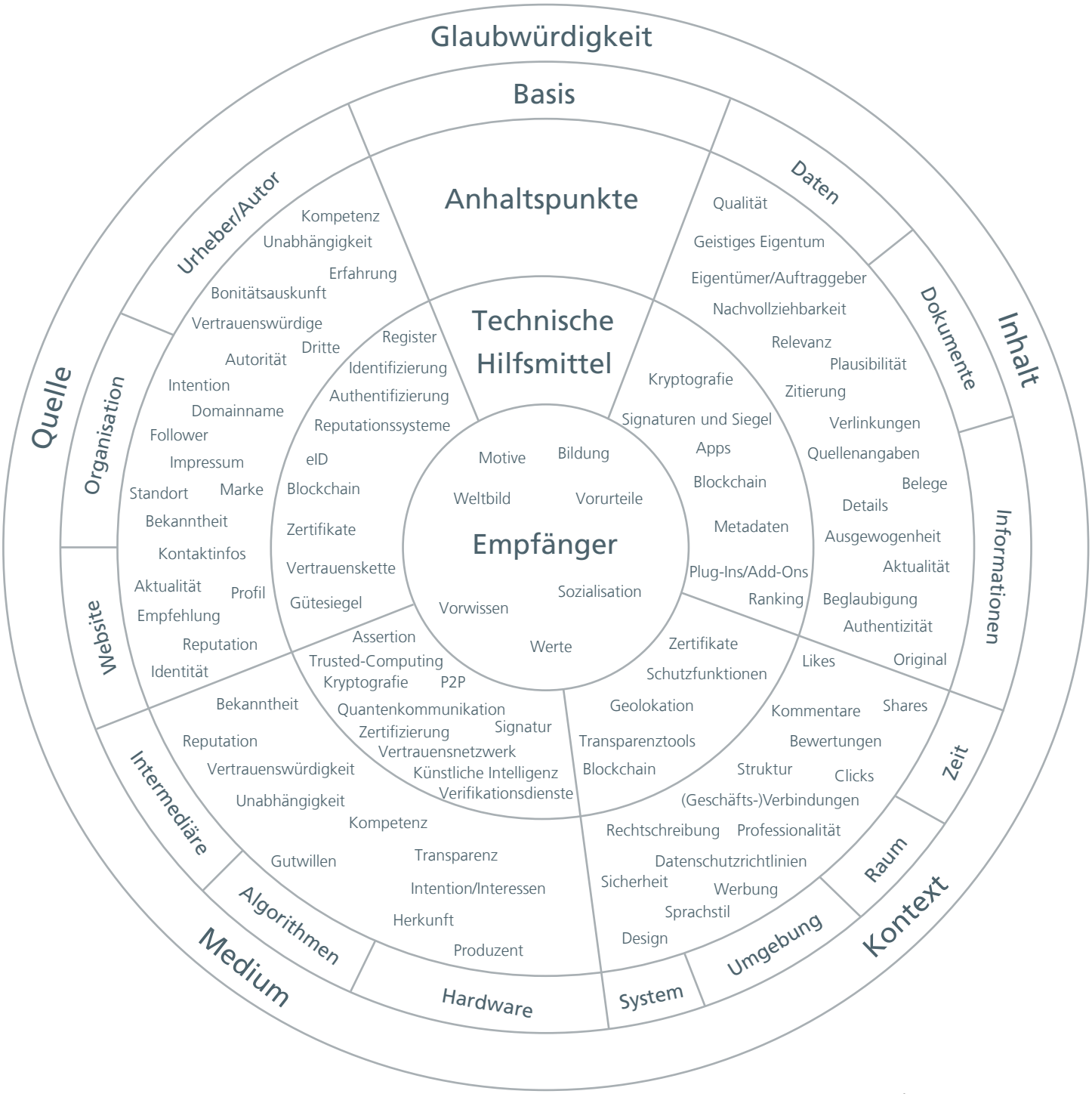

Abbildung 3: Modell für digitale Glaubwürdigkeit

4. TECHNISCHE KONZEPTE, METHODEN UND LÖSUNGSANSÄTZE

So unterschiedlich die Dimensionen für Glaubwürdigkeit sind, nämlich Quelle, Inhalt, Kontext und Medium und Empfänger im Modell für digitale Glaubwürdigkeit (vgl. Abbildung 3), so unterschiedlich sind auch die Anhaltspunkte für deren Beurteilung. Technische Konzepte, Methoden und Lösungsansätze können die digitale Glaubwürdigkeit stärken. Allerdings ist auch eine böswillige oder unachtsame Schwächung der Glaubwürdigkeit durch falsche Informationen und Daten, gefälschte Webauftritte oder Online-Shops, Plagiate oder Inkompetenz vermehrt zu beobachten. Das virtuelle Wettrüsten zwischen Mechanismen, die Glaubwürdigkeit stärken, und denen, die sie schwächen, ähnelt dem zwischen Angreifern und Verteidigern in der Informationssicherheit. Glaubwürdigkeit ist wie auch Informationssicherheit kein fixer Zustand, sondern muss ständig kontrolliert und verbessert werden.

4.1 REPUTATION UND BEWERTUNGSSYSTEME

In Online-Umgebungen hat man es häufig mit Unbekannten zu tun. Als Ersatz für die fehlenden eigenen Erfahrungen mit seinem Gegenüber liefert die Reputation – früher auch als der »gute Ruf« bezeichnet – einen Anhaltspunkt für deren Verhaltensweise. Die Glaubwürdigkeit eines Geschäftspartners oder einer Privatperson basiert dabei auf deren Verhalten in der Vergangenheit. Dieses wird in die Zukunft projiziert, um Vertrauen zu schaffen oder zu erhalten, das heißt positives Verhalten in der Vergangenheit lässt darauf schließen, dass auch in der Zukunft das Verhalten positiv ist. Gemessen wird die Glaubwürdigkeit mit unterschiedlichen Kennzahlen und Methoden.

Fast jedem Nutzer sind Bewertungssysteme in Online-Portalen und -Plattformen wie etwa bei Google, Ebay, Amazon, Ciao oder TripAdvisor bekannt. Sterne, Punkte, Smileys, Daumen, Schulnoten und andere Kennzahlen repräsentieren die Meinung anderer Nutzer bezüglich einer Person, einer Organisation, eines Produktes oder Vorganges auf einen Blick. Häufig sind auch textuelle Bewertungskommentare zusätzlich möglich.

Traditionelle Auskunfteien (bspw. Schufa, creditreform oder infoscore) analysieren mit geheimen Algorithmen personenbezogene und andere Daten (deren Art und Herkunft teilweise ebenfalls geheim sind) und stellen die Bewertung zahlenden Anfragern zur Verfügung. Dies wird durch Medien und Verbraucherschützer häufig kritisiert, insbesondere da die Bewerteten nicht erfahren, wie sie einen ungünstigen Score verbessern können. In Online-Portalen werden dagegen die Kunden nach ihrer Bewertung gefragt. Doch was wird eigentlich bewertet? Ist es das Produkt, die Plattform, der Verkäufer, der Verkaufsprozess, die Logistik oder das Lager? Neutralität, Objektivität und Vergleichbarkeit sind keine Kriterien, sondern die Masse der Bewertungen und ihre einfache Darstellung im Web sind gefragt. Der Grund für diese Vorgehensweise ist einfach: Viele gute Bewertungen sind in ihrer Masse vertrauenswürdig und erhöhen Bekanntheit, Umsatz und Verbreitung sowie die Glaubwürdigkeit und Vertrauenswürdigkeit. Sie stellen die wichtigste Kaufhilfe dar.[21] Im Umkehrschluss bedeutet das: Unternehmen, die Ihre Produkte online vertreiben, haben das Ziel, eine möglichst große Anzahl positiver Bewertungen zu erhalten. Dieser Umstand bringt allerdings ganz neue Geschäftszweige hervor.

Fake-Bewertungen

Fake-Bewertungen und falsche Meinungsäußerungen (Opinion Spam) freuen den einen oder schädigen den anderen. Die Macht der Bewertungen fördert auch deren Fälschungen, unter anderem durch gekaufte Rezensionen. Die Bandbreite der Fälschungen variiert dabei von ein bisschen Schummeln bis zu kriminellen Machenschaften.

Verschiedene Beispiele verdeutlichen die Fälschungsproblematik: Etwa ein Drittel der Online-Bewertungen auf Reiseportalen ist beauftragt oder gefälscht.[22] 20 - 30 Prozent der Bewertungen sind auch bei Amazon gefälscht, berichtet Galileo.tv.[23] Bei unseriösen Agenturen oder Personen im In- oder Ausland kostet eine Falschbewertung 4 - 6 Euro. Krimineller und daher teurer sind mit ca. 25 Euro falsche Bewertungen der Konkurrenz, um diese zu schädigen. In den USA geht Amazon daher gegen die

[21] Bitkom, Kundenbewertungen sind wichtigste Kaufhilfe 11.01.2017, https://www.bitkom.org/Presse/Presseinformation/Kundenbewertungen-sind-wichtigste-Kaufhilfe.html.

[22] Hans-Werner Rodrian, So erkennt man Betrug auf Reise-Portalen, 23.9.2017, https://www.abendblatt.de/reise/article212017277/So-erkennt-man-Betrug-auf-Reise-Portalen.html.

[23] Galileo.tv, So werden Kundenbewertungen für Online-Shops manipuliert, Pro7 18.12.2016, https://www.galileo.tv/video/sonntag-so-werden-kundenbewertungen-fuer-online-shops-manipuliert/.

NEUE METHODEN FÜR DIE GENERIERUNG VON REPUTATIONSDATEN NUTZEN ZUNEHMEND BIG DATA.

Verfasser gefälschter Produktrezensionen gerichtlich vor, um Schaden von der Glaubwürdigkeit seines Bewertungssystems abzuwenden.[24] Auch andere Plattformen sind ständig bestrebt, ihre Bewertungssysteme zu verbessern und gegen Betrug zu schützen. Das Antibetrugsteam bei TripAdvisor arbeitet mit einem geheimen Algorithmus. Bestimmte Merkmale sind jedoch bekannt: Wenn etwa für ein Hotel in Bayern überdurchschnittlich viele Kommentare von IP-Adressen aus einem fernen Staat versendet werden und diese auch bei anderen deutschen Hotels auftauchen, wird Betrug durch eine Agentur im Herkunftsstaat der Kommentare vermutet.[25] Auch Ebay experimentiert schon seit Jahren mit seinem Bewertungssystem: Seien es die Abschaffung der negativen Käuferbewertung durch den Verkäufer, das Einbeziehen nur der letzten zwölf Monate in die Verkäuferbewertung oder gar die Abschaffung der Bewertung insgesamt und etwa der Käuferschutz als Alternative.

Fakes sind auch in den sozialen Medien nicht unbekannt. Fake »Follower« etwa bei Twitter oder Instagram können ebenfalls gekauft werden, um die eigene Reputation zu steigern. Es existieren auch hierfür Dienstleister, die falsche Follower Accounts erstellen oder Aktivitäten mit Social Bots automatisieren.[26]

Wie erkennt man gefälschte Kundenbewertungen? Es gibt verschieden Anhaltspunkte, wie sehr detaillierte Beschreibungen, Käufer, die immer in der gleichen Produktkategorie bewerten, Werbe-Slang oder blumige Sprache. Auch sind sogenannte Produkttester zweifelhaft, die kostenlos Produkte zur Verfügung gestellt bekommen, um diese zu bewerten.[27] Um sich nicht selbst mit diesen Beurteilungen auseinandersetzen zu müssen, existieren hier auch bereits Dienstleister, wie etwa ReviewMeta[28], welche Bewertungen technisch durch Algorithmen auf Glaubwürdigkeit analysieren.[29]

Transferieren von Reputationsdaten

Häufig besteht bei Unternehmen oder Personen der Wunsch, ihre Reputation auch in andere Online-Plattformen und -Portale zu transferieren. Dafür existieren verschiedene Lösungsvarianten:

- Bewertungen von verschiedenen Plattformen werden in einem Siegel zusammengefasst. Dabei bleibt erkennbar, welche Bewertung von welchem Portal stammt. (Beispiel Trustami[30]).
- Bewertungen werden von anderen Plattformen importiert und auf der neuen Plattform dargestellt (Beispiel TrustedShops[31]).
- Bewertungen aus Plattformen, Fragebögen oder auch Kommentaren in sozialen Medien werden ermittelt und mittels Algorithmen wird eine neue übergreifende Bewertungskennzahl errechnet (Beispiel TrustYou[32]).

[24] Virginia Kirst, Amazons verzweifelter Kampf gegen Fake-Rezensionen 19.10.2015, https://www.welt.de/wirtschaft/article147784336/Amazons-verzweifelter-Kampf-gegen-Fake-Rezensionen.html.

[25] Caterina Lobenstein, Schön geschummelt, Viele Hotelbewertungen im Netz sind Eigenlob. Aber welche? 25.7.2013, http://www.zeit.de/2013/31/gefaelschte-online-bewertungen.

[26] Jan Dennis Gumz/Resa Mohabbat Kar, Social Bots, ÖFIT-Trendschau, Kompetenzzentrum Öffentliche IT, Fraunhofer FOKUS Juli 2017, http://www.oeffentliche-it.de/trendschau.

[27] Cornelia Karin Hendrich, So erkennen Sie gefälschte Kundenbewertungen, 21.03.2017, https://www.welt.de/wirtschaft/article162950671/So-erkennen-Sie-gefaelschte-Kundenbewertungen.html.

[28] ReviewMeta, Amazon Review Checker, https://reviewmeta.com/.

[29] Thomas Klemm, Amazon-Bewertungen im Check 30.1.2017, http://www.faz.net/aktuell/finanzen/schutz-vor-missbrauch-fuer-amazon-bewertungssystem-14781041.html.

[30] Trustami: https://app.trustami.com/.

[31] Trustedshops: https://business.trustedshops.de/blog/bewertungen-importieren-trusted-shops/.

[32] TrustYou: http://www.trustyou.com/.

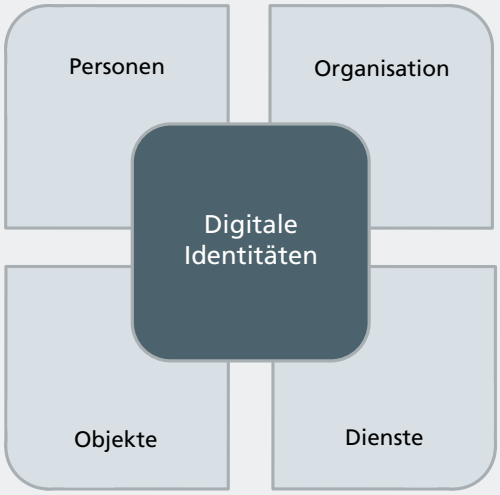

Abbildung 4: Verschiedene Typen digitaler Identitäten[39]

Neue Methoden der Bewertung basieren nicht nur auf Kommentaren von anderen, sondern nutzen zunehmend Big Data. Zwei Beispiele verdeutlichen das:

- Kreditech[33] analysiert und bewertet die Kreditwürdigkeit von Menschen in Echtzeit mit selbstlernenden Algorithmen anhand verschiedenster Arten von Daten wie etwa Standort, soziale Medien (Freunde, Likes, Kommentare), Verhaltensanalysen wie Verweildauer auf Websites, genutzte Hardware und Software (Betriebssystem oder Browser) und Kaufverhalten.
- Klout[34] misst und bewertet die digitale Bedeutung und den Einfluss von Menschen mit ca. 400 geheimen Einzelfaktoren und deren Kombinationen aus acht Netzwerken wie u. a. der Freundesanzahl, Weiterempfehlungen und Reaktionsquote in sozialen Netzwerken im Verhältnis zu den geteilten Inhalten. Daraus wird der Klout-Score (1 bis 100) berechnet. Je mehr ein Mensch andere zum Handeln bewegen kann, umso höher ist der Wert. Ob ein hoher Klout-Score auch eine hohe Reputation darstellt und Menschen glaubwürdiger erscheinen lässt, ist jedoch noch zweifelhaft.

Datenportabilität (Recht auf Datenübertragbarkeit) wird auch in der europäischen Datenschutz-Grundverordnung[35] im Artikel 20 geregelt. Personenbezogene Daten von Nutzern, die diese Firmen oder Behörden zur Verfügung stellen, müssen den Nutzern in strukturierter und maschinenlesbarer Form zurückgegeben werden können, um sie bei Bedarf anderen Dienstleistern zu übermitteln. Noch besteht Unklarheit, wie dieses Recht technisch umgesetzt werden soll. Allerdings besteht die rechtliche Auffassung, dass dies nicht die Daten betrifft, die durch Bearbeitungsschritte aufseiten der Unternehmen berechnet werden. Somit müssen die Ergebnisse von Big-Data-Analysen oder Scorings nicht zur Verfügung gestellt werden.[36]

4.2 VERTRAUENSWÜRDIGE IDENTITÄTEN

»On the Internet, nobody knows you're a dog«[37] wurde schon 1993 als Spruch unter einem Cartoon veröffentlicht. Wie glaubwürdig ist eine digitale Identität heute? Digitale Identitäten[38] werden durch eine Menge von Attributen charakterisiert. Wie auch in der realen Welt repräsentieren die Attribute Eigenschaften, Merkmale oder Präferenzen (Vorlieben, Interessen etc.) der ihr zugrunde liegenden Entität. Digitale Identitäten können sich über ihren Lebenszyklus hinweg verändern und dabei direkt oder indirekt, mit und ohne Wissen des Inhabers erstellt werden. Eine Entität kann mehrere Teilidentitäten besitzen, die je nach Kontext eingesetzt werden, wie beispielsweise »über 18« oder »Führerscheininhaber«. Bei Personenidentitäten sind zudem im digitalen Raum Wunschidentitäten zu finden, die von der realen Welt abweichen können und dann, an bestimmten Stellen eingesetzt, ebenfalls eine Facette von Fake darstellen.

[33] Kreditech: https://www.kreditech.com/ ; siehe auch Wikipedia https://en.wikipedia.org/wiki/Kreditech.

[34] Klout: https://klout.com/, Siehe auch Spiegel Online: http://www.spiegel.de/karriere/klout-wird-bei-personalern-immer-beliebter-a-897527.html.

[35] EU-Datenschutz-Grundverordnung vom 27. April 2016, http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679.

[36] Schürmann Wolschendorf Dreyer Rechtsanwälte, Datenportabilität: Neue Rechte durch die Datenschutzgrundverordnung, 20.4.2017, http://www.swd-rechtsanwaelte.de/blog/recht-auf-datenportabilitaet_dsgvo/.

[37] Wikipedia, https://en.wikipedia.org/wiki/On_the_Internet,_nobody_knows_you%27re_a_dog.

[38] Definition: Eine Identität ist eine Menge von Identitätsattributen, die einer Entität zugeordnet sind. Eine Entität kann mehrere Identitäten haben, ebenso können mehrere Entitäten die gleiche Identität haben. Eine Identität ist daher im Allgemeinen nicht eindeutig, kann dies aber in einem bestimmten Anwendungskontext sein. (BSI TR-03107-1, 31.10.2016, https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03107/index_htm.html).

[39] Jens Fromm, Christian Welzel, Petra Hoepner, Jonas Pattberg, Vertrauenswürdige digitale Identität: Baustein für Öffentliche IT, Oktober 2013, http://www.oeffentliche-it.de/publikationen?doc=14686&title=Vertrauensw%C3%BCrdige+digitale+Identit%C3%A4t+Baustein+f%C3%BCr+%C3%B6ffentliche+IT.

Installationen des Lügenmuseums von Reinhard Zabka.

Im Kontext der Digitalisierung spielen digitale Identitäten eine zentrale Rolle. Wann immer Personen, Organisationen, Objekte oder Dienste miteinander kommunizieren, werden Mechanismen für sichere und vertrauenswürdige Identitäten benötigt, damit man diesen glauben kann.

Wesentlich für die Glaubwürdigkeit von digitalen Identitäten sind deren Identifizierung und die Prüfung der bereitgestellten Identitätsattribute. Werden beispielsweise Online-Konten für Personen nur aufgrund von Eigenangaben ohne deren Validierung erstellt, so ist deren Glaubwürdigkeit als gering einzustufen. Im Gegensatz dazu sind Attribute aus dem Personalausweis, die mit der Online-Ausweisfunktion übermittelt werden, authentisch[40]. Authentizität ist das wesentliche Kriterium für Glaubwürdigkeit und die Grundlage für den Aufbau von Vertrauensbeziehungen und die Wiedererkennung von Nutzern oder auch anderen Objekten.

Nach Abschluss einer Identifizierung und Registrierung werden meist Authentisierungsmittel[41] (Passwörter, Chipkarte/PIN, Softwarezertifikate etc.), vergeben oder übermittelt, die das Wiedererkennen einer digitalen Identität (Authentisierung) in der Online-Umgebung ermöglichen. Nur wenn sowohl Identifizierung und Registrierung als auch Authentisierung sicher und vertrauenswürdig erfolgen, ist die digitale Identität ebenfalls authentisch und daher glaubwürdig.

Authentizität erfordert jedoch nicht die vollständige Offenlegung persönlicher Daten. Pseudonymität oder Anonymität sind in bestimmten Anwendungskontexten aus Datenschutzgründen erlaubt oder sogar erforderlich. Glaubwürdigkeit muss dann aus anderen Identifikationsattributen im betreffenden Kommunikationskontext abgeleitet werden.

4.3 SIEGEL UND ZERTIFIKATE

Um Glaubwürdigkeit zu stärken, werden in verschiedenen Bereichen Siegel und Zertifikate verwendet. Generell dienen Zertifikate und Siegel dem Nachweis bestimmter Eigenschaften, sie sollen die Transparenz erhöhen und Vertrauen bei den Nutzern und Anwendern erzeugen.

Für die IT-Sicherheit sind Zertifikate und Anerkennungen für Produkte, Managementsysteme, Personen, Prüfstellen und Dienstleister nach festgelegten Kriterien und Verfahren schon lange etabliert. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat nach dem BSI-Gesetz und der BSI-Zertifizierungsverordnung die Aufgabe, bestimmte Zertifizierungen durchzuführen und betreibt entsprechende Zertifizierungsprogramme. Jede Zertifizierung basiert auf einem Regelwerk, das die Geltungsbereiche, bedarfsgerechten Prüfkriterien, Anforderungen und Nachweise beschreibt und das Verfahren sowie das Management zur Durchführung der Zertifizierung festlegt. Ein bekanntes Beispiel hierfür sind die Common Criteria[42] (CC) für IT-Sicherheitszertifikate. Anhand des Regelwerkes wird die Vertrauenswürdigkeit (Evaluation Assurance Level, EAL-Stufe) einer Sicherheitsleistung zertifiziert.

[40] Der Duden definiert »authentisch« als »echt; den Tatsachen entsprechend und daher glaubwürdig«.

[41] Definition: Authentisierungsmittel sind technische Mittel, die es dem Inhaber erlauben, eine Identität (das heißt eine Menge von Identitätsattributen) oder andere übermittelte Daten zu authentisieren. Beispiele für Authentisierungsmittel sind Passwörter, der Personalausweis oder kryptographische Token. Sind mehrere technische Mittel notwendig (etwa Chipkarte und PIN), so besteht das vollständige Authentisierungsmittel aus mehreren Authentisierungsfaktoren. (BSI TR-03107-1, 31.10.2016, https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03107/index_htm.html).

[42] CC, Common Criteria for Information Technology Security Evaluation, Version 3.1, http://www.commoncriteriaportal.org.

JEDER KANN GÜTE- UND PRÜFSIEGEL ERFINDEN, DA ES KEINE GESETZLICHEN REGELUNGEN GIBT.

Auch die EU-eIDAS-Verordnung[43] regelt elektronische Signaturen für Personen und Siegel für Organisationen basierend auf qualifizierten Signatur- und Siegelzertifikaten. Diese Zertifikate sind elektronische Bescheinigungen, die Validierungsdaten mit einer natürlichen oder juristischen Person verknüpfen und die mindestens den Namen dieser bestätigen. Trust Center, die diese Zertifikate ausstellen dürfen, müssen in Deutschland der Technischen Richtlinie TR-03145[44] des BSI entsprechen.

Neben diesen Siegeln und Zertifikaten existiert eine Vielzahl von Gütesiegeln aller Art, um qualitative Eigenschaften von Produkten, Websites, Geschäften, Dienstleistungen etc. zu bescheinigen. Allerdings wird hier schon deutlich, dass man sich fragen muss: »Wer bescheinigt was, wofür und nach welchen Regeln?« In den oben genannten Beispielen hingegen bilden Regelwerke und vertrauenswürdige Aussteller die Grundlage. Nach einer Umfrage[45] zu den Faktoren, welche die Glaubwürdigkeit von Gütesiegeln beeinflussen, sind die wichtigsten drei Faktoren mit jeweils mehr als 66 Prozent Zustimmung: die Unabhängigkeit des Testinstituts, die Angaben zum Gesamtergebnis bzw. zu anderen getesteten Produkten und die Transparenz der Einflussfaktoren zur Bestimmung des Testurteils.

Da es keine gesetzlichen Regelungen gibt, kann jeder Güte- und Prüfsiegel erfinden. Im Digitalen ist das besonders einfach. Einerseits führt das zu einem Wirrwarr an Siegeln und andererseits werden seriöse Siegel und Zertifikate auch gefälscht und missbraucht. Daraus entstehen Unsicherheiten und folglich Glaubwürdigkeitsprobleme. Aus diesen Gründen sollte auf Webseiten eine Verlinkung zum Aussteller von Siegeln und Zertifikaten erfolgen, der dann weitere Informationen bereitstellt. Ob dieser Aussteller allerdings unparteiisch agiert, transparente und objektive Prüfverfahren anwendet, Nachprüfungen vornimmt und den Kontext der Gültigkeit genau festlegt, bleibt offen, und die Feststellung erfordert häufig detektivisches Gespür und eigene Recherchen der Verbraucher.

Verschiedene Dienstleister haben sich daher das Ziel gesetzt, die Glaubwürdigkeit von Siegeln und Zertifikaten zu erhöhen und Fehlwahrnehmungen zu minimieren. Ein Beispiel ist Siegelklarheit.de[46] (auch als App verfügbar vom Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung). Siegel werden hinsichtlich ihrer Aussage bzgl. Umwelt und Sozialem und hinsichtlich ihrer Glaubwürdigkeit bewertet und können miteinander verglichen werden. Laut der Bewertungsmethodik von Siegelklarheit gibt es für den Bereich Glaubwürdigkeit rund 100 Anforderungen[47]: etwa zum Management der Organisation, die Siegel vergibt, zu den inhaltlichen Anforderungen an das Produkt oder den Produktionsprozess, zum Kontrollsystem und zu den Regeln zur Verwendung des Siegels.

4.4 PEER-TO-PEER-ANSÄTZE

Um Attribute nachzuweisen, Zertifikate auszustellen, Kommunikationspartner zu vermitteln oder Systeme zu kontrollieren, werden häufig zentrale glaubwürdige Instanzen eingeschaltet. Verschiedene Begriffe wie Trust Center, vertrauenswürdiger Dritter, Intermediär oder Broker kennzeichnen diese traditionellen, hierarchischen Autoritäten.

[43] EU-Verordnung Nr. 910/2014 vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG, http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32014R0910.

[44] BSI, TR-03145, https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03145/index_htm.html.

[45] Statista, Umfrage zu Glaubwürdigkeitsfaktoren für Gütesiegel in Deutschland 2013, https://de.statista.com/statistik/daten/studie/273350/umfrage/umfrage-zu-glaubwuerdigkeitsfaktoren-fuer-guetesiegel-in-deutschland/.

[46] Siegelklarheit.de, https://www.siegelklarheit.de/home.

[47] Bewertungsmethodik, https://www.siegelklarheit.de/bewertung/.

SOFTWARE-GENERIERTE NACHRICHTEN WERDEN VON LESERN HÄUFIG ALS GLAUBWÜRDIGER WAHRGENOMMEN ALS VON MENSCHEN GESCHRIEBENE TEXTE.

Als Gegensatz dazu ist der Peer-to-Peer-Ansatz (P2P) einzuordnen. Generell sind darunter dezentrale Systeme zu verstehen, in denen Gleichberechtigte interagieren. Glaubwürdigkeit und Vertrauenswürdigkeit in diesen Systemen erfordert auch ein dezentrales Modell.

Ein Beispiel ist PGP (Pretty Good Privacy) zum Verschlüsseln und Signieren basierend auf Zertifikaten, die nicht von einer zentralen Zertifizierungsinstanz ausgestellt werden. Das Vertrauen zwischen den Benutzern wird durch ein dezentrales Modell, das Web of Trust[48/49] geregelt. Dabei bestimmen die Nutzer gegenseitig, wer aus ihrer Sicht vertrauenswürdig ist und welchem Schlüssel und somit welcher Identität sie glauben. So entstehen Vertrauensketten zwischen einander Unbekannten über Zweierbeziehungen einander vertrauender Nutzer. Eine aktuelle Ausprägung eines Peer-to-Peer-Ansatzes ist die Blockchain.

Blockchain

Unter einer Blockchain versteht man ein verteiltes, dezentrales Register (auch als Datenbank bezeichnet), das Transaktionen in chronologischer Reihenfolge unveränderbar und nachvollziehbar speichert und miteinander verkettet. Wesentlich ist, dass Transaktionen zwischen beliebigen Teilnehmern ohne Zwischenschalten einer kontrollierenden, vertrauenswürdigen Instanz sicher durchgeführt werden können. Überall dort, wo heute zentrale Instanzen Glaubwürdigkeit und Vertrauen in Prozessabläufe bringen, stellt die Blockchain eine technische Alternative dar. Die klassischen Funktionen eines Intermediärs – Protokollierung, Prozessdurchführung und Transaktionsabsicherung – werden dabei durch eine geschickte Kombination vorwiegend technischer Verfahren bestehend aus Kryptografie (digitalen Signaturen), der rechenintensiven Lösung situationsabhängiger Kodierungsaufgaben und P2P-Netzwerken abgesichert.[50] Die potenziellen Anwendungsbereiche sind vielfältig und sollen typische Intermediäre (teilweise) ersetzen können, wie etwa Banken, Notare, Behörden oder Plattformen.

Beispielsweise könnte nachgewiesen werden, dass ein Dokument zu einer bestimmten Zeit einer bestimmten Person oder Organisation in einer bestimmten Fassung vorgelegen hat. Dazu wird der zugehörige Hashwert[51] des Dokuments in der Blockchain von diesem Teilnehmer unveränderbar und dauerhaft gespeichert. Weitere Anwendungsszenarien finden sich für Nachweisprotokolle, um Produktions- oder Lieferketten zu bezeugen, etwa wenn es um die Verwendung oder die Herkunft von Produkten geht.

Nicht nur für Dokumente, auch für einzelne Daten kann die Integrität[52] über eine Blockchain geprüft werden. Erste Prototypen existieren beispielsweise für die Abbildung digitaler Identitäten. Hierbei werden Hashwerte über eine Menge von Identitätsattributen gebildet und in einer Blockchain abgelegt. Auch hierbei geht es darum, die Integrität der Identitätsattribute sicherzustellen.

[48] Dieses Modell liegt beispielsweise auch den Erfahrungsberichten in der Internet Community Ciao zugrunde. Mitglieder können ein »Netz des Vertrauens« aufbauen, um Erfahrungsberichte von den von ihnen als glaubwürdig eingestuften Mitgliedern am Anfang der Liste von Beiträgen zu sehen. http://www.ciao.de/faq/netz-des-vertrauens-nutzen.

[49] Nicht zu verwechseln mit der Browser-Erweiterung und Bewertungsplattform »Web of Trust«. Diese ist durch die Weitergabe von Nutzerdaten negativ aufgefallen. Tagesschau.de, »Web of Trust späht Nutzer aus«, 1.11.2016, https://www.tagesschau.de/inland/tracker-online-103.html.

[50] Christian Welzel u. a., Mythos Blockchain: Herausforderung für den öffentlichen Sektor, März 2017, http://www.oeffentliche-it.de/publikationen.

[51] Ein Hashwert ist eine Zeichenfolge fester Länge, die mittels einer mathematischen Funktion (sog. Hashfunktion) aus einem beliebig langen Text gebildet wird. Verändert sich ein Zeichen des ursprünglichen Textes, ergibt das einen anderen Hashwert. Von einem Hashwert kann nicht auf den ursprünglichen Text geschlossen werden.

[52] Integrität von Daten bedeutet, dass diese unversehrt sind, d. h. nicht manipuliert wurden.

Titanic-oder-Narrenschiff und die Psychedelica Maschinka (dahinter) im Lügenmuseum.

Ebenfalls können Identitätsattribute durch den Benutzer, andere Berechtigte oder durch eine als Autorität anerkannte Stelle bestätigt werden (wird auch als Attestierung bezeichnet). Anwendungen wie »Bring Your Own Identity« statt Nutzernamen und Passwörtern für den jeweiligen Anwendungskontext erscheinen möglich.[53]

4.5 ALGORITHMEN

Algorithmen werden heutzutage häufig in Zusammenhang mit Big Data, denkenden Maschinen und selbstlernender künstlicher Intelligenz genannt. Ihnen haftet daher etwas Unverständliches, Überwachendes und Unheimliches an. Das ist allerdings ein Trugschluss. Grundsätzlich ist ein Algorithmus nur eine eindeutige Handlungsvorschrift zur Lösung eines Problems oder einer Klasse von Problemen bestehend aus Einzelschritten.[54] Werden diese Algorithmen in einer Programmiersprache verfasst, d. h. implementiert, können Computer diese ausführen.

Algorithmen werden von Menschen erdacht, können einfach oder extrem komplex sein und erfüllen unterschiedliche Zielkriterien. Mit einem Algorithmus wird somit immer ein Stück fremdes Denken übernommen.[55/56] Glaubwürdigkeit kann daher bezüglich Algorithmen unterschiedlich ausgelegt werden:

– *Algorithmen als Quelle:* Algorithmen können als Quelle von Daten aller Art auftreten. Dabei können diese etwa gesammelt, analysiert oder verarbeitet werden. Glaubwürdigkeit ist hier abhängig von den ursprünglichen Quellen und von der Qualität der verarbeitenden Algorithmen. Als Beispiel ist Roboterjournalismus zu nennen. Sogenannte Textroboter (Software) generieren Nachrichten (etwa Sport- oder Finanznachrichten) aus Daten, Worten und Textbausteinen aus verschiedenen Datenbanken oder Echtzeitmedien. Von Lesern werden diese häufig glaubwürdiger wahrgenommen als von Menschen geschriebene Texte, da sie viele Zahlen und detaillierte Fakten enthalten.[57] Ähnliche Versuche haben auch gezeigt, dass Roboter (Hardware) als glaubwürdig eingeschätzt werden. So folgten in einem fingierten Brandfall Versuchspersonen einem Roboter, der sich als Notfallführer ausgab, statt den ihnen bekannten Weg zu nutzen, auf dem sie gekommen waren. In einem anderen Fall gossen sogar drei Viertel der Probanden auf Aufforderung des Roboters Orangensaft auf eine Topfpflanze und neunzig Prozent warfen ungeöffnete Briefe eines fingierten Gastgebers in den Papierkorb.[58] Ein kritischen Hinterfragen der eigenen Aktivitäten fand nur eingeschränkt statt (»Ich dachte, der Roboter versteht mehr von Botanik als ich«), was zeigt, dass die Anweisungen der Roboter glaubwürdig erschienen, obwohl sie unsinnig waren.

[53] TeleTrusT, TeleTrusT-Positionspapier »Blockchain«, Handreichung zum Umgang mit der Blockchain, https://www.teletrust.de/publikationen/broschueren/blockchain/.

[54] Wikipedia, Algorithmus, https://de.wikipedia.org/wiki/Algorithmus.

[55] Viktoria Bittmann, Algorithmen treffen ins Mark der Macht 9.1.2017, https://www.politik-kommunikation.de/ressorts/artikel/algorithmen-treffen-ins-mark-der-macht-93003943.

[56] BLM (Hrsg.), Dein Algorithmus – meine Meinung!, Algorithmen und ihre Bedeutung für Meinungsbildung und Demokratie, Bayerische Landeszentrale für neue Medien, München 2017, https://www.blm.de/files/pdf1/algorithmen_broschuere.pdf.

[57] Andreas Graefe, Mario Haim, Bastian Haarmann, Hans-Bernd Brosius, Readers' perception of computer-generated news: Credibility, expertise, and readability, http://journals.sagepub.com/doi/10.1177/1464884916641269.

[58] Manuela Lenzen, Lassen Sie sich von seinem Lächeln nicht täuschen!, Vertrauen in Roboter, http://www.faz.net/aktuell/feuilleton/forschung-und-lehre/vertrauen-in-roboter-lassen-sie-sich-von-seinem-laecheln-nicht-taeuschen-14454603.html.

Installationen des Lügenmuseums von Reinhard Zabka

– *Algorithmen als technisches Hilfsmittel zur Beurteilung der Glaubwürdigkeit von Quellen:* Algorithmen können die Aufdeckung von Fake News unterstützen. Beispielsweise werden manipulierte Bilder von Menschen kaum erkannt.[59] Intelligente Algorithmen, wie etwa das Browser-Add-on »News Verifier«, erkennen über einen Bildidentifikationsalgorithmus Manipulationen anhand inhaltlicher Veränderungen zu ähnlichen Fotos.[60]
– *Algorithmen zur Beeinflussung der Glaubwürdigkeit beim Empfänger:* Algorithmen können auch Fakes erzeugen. Social Bots etwa können zur gezielten Verbreitung von Falschinformationen (z. B. Glaubwürdigkeit durch Masse) eingesetzt werden – mit entsprechenden Möglichkeiten zur Desinformation, Täuschung und Manipulation von Meinungsbildungsprozessen.[61] Ebenfalls sind kaskadierende Effekte durch Hintereinanderschalten von Algorithmen möglich, wenn deren Glaubwürdigkeit nicht verifiziert wird. So können etwa Falschangaben über Firmen durch Textroboter zu Aktienkäufen führen, wenn Finanzalgorithmen diese ungeprüft übernehmen.

Komplexe Algorithmen sind auch die Grundlage für Künstliche-Intelligenz-Systeme (KI-Systeme). Die Datenbasis dieser Systeme wird entweder von Menschen aufbereitet oder die Systeme »lernen«. Maschinelles Lernen erfordert Trainingsdaten. Beispielsweise wird die Fähigkeit, einen Baum zu erkennen, anhand einer Vielzahl von Trainingsdaten in Form von beschriebenen Bildern mit und ohne Baum geübt. Die Auswahl der Trainingsdaten bildet also neben den Algorithmen die Grundlage für glaubwürdige Ergebnisse. Unvollständige oder unpassende Daten liefern unerwünschte Ergebnisse. Die konkrete Arbeitsweise dieser komplexen Systeme gleicht einer Black Box, die im Optimalfall genau das tut, was sie soll, aber ihr Arbeitsprinzip nicht preisgibt.[62]

4.6 TOOLS UND ANWENDUNGEN FÜR PLATTFORMEN UND SOZIALE NETZWERKE

Um Fake schneller zu enttarnen, werden verschiedene Tools zur Unterstützung angeboten. Grundlage dieser Tools sind wiederum Algorithmen, die eine Vielzahl von Indikatoren analysieren und bewerten, wie etwa bestimmte Eigenschaften des zu überprüfenden Objekts, dessen Kontext und/oder Herkunft. Beispiele sind:

– ReviewMeta[63] ist ein Unterstützungstool, um manipulierte Kundenbewertungen bei Amazon zu entdecken und die Sterneangabe der Produktbewertung zu korrigieren. ReviewMeta untersucht verschiedene Eigenschaften einer Bewertung, z. B.: Hat der Verfasser schon mal ein Review verfasst? Ist er ein verifizierter Käufer? Gibt es unnatürlich viele Bewertungen vom gleichen Tag? Ähneln sich Aufbau und Wortwahl von Bewertungen?

[59] Florian Rötzer, Können Menschen manipulierte »Fake-Bilder« erkennen?, 25.7.2017, https://heise.de/-3782064.

[60] DFKI, Wenn die Bilder lügen –KI-System entlarvt Fake News im Internet, 20.4.2017, https://www.dfki.de/web/presse/pressemitteilung/2017/newsverifier.

[61] J. D. Gumz / R. M. Kar (Anm. 26).

[62] Dorian Grosch, Neuronale Netze, ÖFIT-Trendschau, Kompetenzzentrum Öffentliche IT, Fraunhofer FOKUS, Juli 2017, http://www.oeffentliche-it.de/trendschau.

[63] ReviewMeta, https://reviewmeta.com/.

DIE MEISTEN SEHEN ALS GLAUBWÜRDIG AN, WAS IHREM EIGENEN DENKEN AM NÄCHSTEN KOMMT.

- WikiTrust[64] ist ein Tool, um Glaubwürdigkeit innerhalb eines Wikipedia-Artikels zu erfassen und farblich differenziert darzustellen. Dabei wird unter anderem von Algorithmen die Vertrauenswürdigkeit der Autoren eingeschätzt. Die als verlässlich angesehenen Inhalte, für die Konsens unter den Autoren des Artikels besteht, stellt WikiTrust normal dar, neue oder fragwürdige Inhalte werden farblich markiert.
- BotOrNot prüft Twitter-Accounts algorithmisch und bewertet anhand von über 1000 Anhaltspunkten, ob diese Menschen oder Social Bots zugehören.[65]
- Google trainiert und verbessert seinen Suchalgorithmus gegen Falschinformationen und menschenverachtende Inhalte mittels menschlicher Bewertungsteams, den Quality Raters, die die Glaubwürdigkeit von Quellen einschätzen.[66]
- Das Auswerten von Metadaten von Bildern oder Videos kann ebenfalls Ungereimtheiten zutage bringen. Tools wie Exif-Viewer oder der Youtube DataViewer unterstützen dabei.
- Facebook will zukünftig im Kampf gegen gefälschte Nachrichten stärker selbstlernende Software einsetzen, die zweifelhafte Inhalte erkennen und als Entscheidungshilfe für Korrekturen dienen soll.[67]

Die Beispiele zeigen, dass es viele verschiedene Bestrebungen gibt, Falschinformationen zu erkennen, zu kennzeichnen, darzustellen oder auch zu löschen. Allerdings werden die meisten Nutzer nur selten entsprechende Tools in Anspruch nehmen. Die meisten sehen als glaubwürdig an, was ihrer eigenen Einstellung am nächsten kommt. Daher wäre das Einführen von Kennzeichnungen für potenziell gefälschte Inhalte durch die verwendeten Dienste, Systeme oder sozialen Medien ein Schritt zur Bewusstmachung möglicher Fälschungen, wie es Facebook beispielsweise erprobt.[68]

[64] Wikipedia, WikiTrust, https://de.wikipedia.org/wiki/WikiTrust.

[65] Clayton Allen Davis u. a., BotOrNot, in: Jacqueline Bourdeau u. a. (Hrsg.), Proceedings of the 25th International Conference Companion on World Wide Web 2016.

[66] t3n (Hrsg.), Gegen Fake-News und Gewalt: So trainiert Google den Suchalgorithmus 15.3.2017, http://t3n.de/news/google-fake-news-gewalt-suchalgorithmus-805035/.

[67] ZDF (Hrsg.), Fake News: Facebook testet lernende Computer 3.8.2017, http://www.heute.de/fake-news-facebook-setzt-auf-lernende-computer-47694340.html.

[68] Daniel Berger, Facebook kennzeichnet »Fake News« 6.3.2017, https://heise.de/-3644733.

Aufbau der Ausstellung »unverbesserlich«, im großen Saal des Lügenmuseums.

5. STRATEGISCHE UND ORGANISATORISCHE VORGEHENSWEISEN

Die digitale Transformation kann nur dann gelingen, wenn authentische, glaubwürdige Daten, Informationen, Dokumente, Produkte, Märkte, Plattformen, Dienste, Teilnehmer und Systeme gewährleistet werden. Unsicherheit und Zweifel behindern sie. Es gilt in allen Bereichen, die Glaubwürdigkeit zu stärken. Dazu dienen neben technischen Mitteln auch verschiedene strategische und organisatorische Vorgehensweisen.

5.1 TRANSPARENZ

Transparenz wird als eine Voraussetzung für Glaubwürdigkeit betrachtet, da sie dazu dient, die Ungewissheit zu reduzieren. Sie kann unterschiedliche Bereiche betreffen, wie etwa Quellen von Produkten, Herstellungsverfahren, Budget für öffentliche Aufgaben, Lobbyregister, eingesetzte Software für IT-Prozesse oder die Weiterverwendung erhobener Daten. Transparenz bedeutet nicht zwangsläufig, dass Geschäftsgeheimnisse oder vertrauliche Informationen preisgegeben werden müssen.

Oftmals wird das Veröffentlichen von Informationen mit Transparenz gleichgesetzt. Glaubwürdigkeit entsteht aber erst dann, wenn die Informationen kontextspezifisch relevant, verständlich, leicht zugänglich und gegebenenfalls auch nachprüfbar sind.

Ein Beispiel sind Lieferketten von Produkten. Glaubwürdigkeit ist hier eng mit der Echtheit der Produkte und der Nachvollziehbarkeit der Verarbeitungs- und Lieferwege verbunden. Besonders wenn Produkte verarbeitet werden, muss auch die Herkunft der Einzelbestandteilte identifizierbar und nachprüfbar sein. Das wird heute unter anderem durch eine Kennzeichnung von Gütern oder Verpackungen erreicht, wie etwa Sicherheitsetiketten, Mikrofarbcodes, digitalen Wasserzeichen, Kopie-Erkennung oder RFID.[69]

Von der Blockchain verspricht man sich, dass Herkunft und Echtheit von Daten für jedermann überprüfbar abgesichert werden können, und so die Glaubwürdigkeit gestärkt wird.[70]

Digitale Informationsplattformen für unterschiedliche Politikbereiche dienen ebenfalls der Transparenz. Bei manchen Plattformen ist jedoch auch deren Betreiber- und Geschäftsmodell relevant. Beispielsweise warnen Verbraucherschützer bei Reiseportalen vor Verflechtungen im Hintergrund, die deren Unabhängigkeit in Frage stellen und somit die Glaubwürdigkeit einschränken.[71]

Auch der Einsatz von Open-Source-Software verbessert aus technischer Sicht die Transparenz von IT-Anwendungen. Oft wird angenommen, dass diese sicherer ist und keine Hintertüren eingebaut worden sind. Das könnte jedoch ein Trugschluss sein[72], wenn keine Verifikation dieser Annahmen erfolgt.

5.2 VERIFIKATION UND VALIDIERUNG

Aussagen zur Korrektheit von Daten, Informationen, Quellen, Datenbanken, Algorithmen, Orten usw. erfordern die Nachweisbarkeit der Korrektheit bzw. die Verifikation und Validierung der Eigenschaften dieser Objekte. Verifikation und Validierung können durch unterschiedliche Mechanismen oder Verfahren je nach Prüfungsgegenstand erfolgen.

Zertifikate und Siegel, die eine Prüfung durch unabhängige Stellen bescheinigen (vgl. Abschnitt 4.3), sind hier genauso zu nennen wie verifizierte Online-Käufer, d. h. Käufer, die ein bestimmtes Produkt erworben haben und erst dann Bewertungen abgeben dürfen.

Im journalistischen Bereich gelten Prinzipien für die Prüfung von Fakten, bevor Informationen veröffentlicht werden. Faktencheck[73] ist ein diesbezügliches journalistisches Konzept. Portale zum Prüfen von Fakten wie der ARD-Faktenfinder[74] sollen die

[69] Wikipedia, Produktpiraterie, Technische Schutzmaßnahmen, https://de.wikipedia.org/wiki/Produktpiraterie.

[70] C. Welzel u. a. (Anm. 50).

[71] Verbraucherzentrale Bundesverband e.V., Portale täuschen Vielfalt vor, Marktwächteruntersuchung zeigt Defizite, 25.2.2016, https://ssl.marktwaechter.de/pressemeldung/buchungs-und-vergleichsportale-bieten-zu-wenig-nutzen-fuer-verbraucher.

[72] Der Heartbleed-Bug in OpenSSL (2014) war eine der schwerwiegendsten Sicherheitslücken. https://www.golem.de/news/openssl-wichtige-fragen-und-antworten-zu-heartbleed-1404-105740.html.

[73] Wikipedia, Faktencheck, https://de.wikipedia.org/wiki/Faktencheck.

[74] ARD-Faktenfinder, http://faktenfinder.tagesschau.de/index.html.

DASS GERÜCHTE ODER LÜGEN VERBREITET WERDEN, ERREICHT DURCH DIGITALE MEDIEN EINE NEUE DIMENSION.

Glaubwürdigkeit von Berichten untermauern. Ebenfalls entstehen Partnernetzwerke, die eine Fakten- und Qualitätskontrolle von Inhalten vorantreiben. Ein Beispiel ist »First Draft«[75], wo Organisationen aus den Bereichen Journalismus, Menschenrechte und Technologie gemeinsam die Quellenprüfung verbessern und auch praktische und ethische Leitlinien zur Verfügung stellen, wie man aus sozialen Medien stammende Inhalte finden, prüfen und veröffentlichen kann.

5.3 UNTERSTÜTZENDE STELLEN

Zentrale Portale und Plattformen, die Informationen und Tools für die Nachprüfung von Informationen oder Quellen bereitstellen, sind sicherlich eine Hilfe im Dschungel der verschiedenen Möglichkeiten, wie beispielsweise:

- Eine internationale Anlaufstelle ist der Verein Mimikama[76], dessen Ziel es ist, Internetmissbrauch, Internetbetrug und Falschmeldungen bzw. Fakes entgegenzuwirken und zu bekämpfen. Fakes kann man melden, diese werden von Mimikama geprüft und recherchiert und gegebenenfalls veröffentlicht.
- Der Wikipedia-Gründer Jimmy Wales hat Wikitribune[77], ein von Wikipedia unabhängiges kommerzielles Projekt, gegründet. Ziel ist die faktenbasierte Berichterstattung. Dafür sollen zukünftig freiwillige Helfer und Journalisten zusammenarbeiten.[78]
- Sogenannte Hoaxes sind Falschmeldungen und Gerüchte, die von vielen als wahr erachtet und daher gutgläubig weiterverbreitet werden. Diese kursieren schon seit über zwanzig Jahren. Kettenbriefe, falsche Virenwarnungen oder sonstige Schauergeschichten sind nur einige Beispiele. Hoaxes kann man auf verschiedenen Webseiten überprüfen. Ein Beispiel ist der Hoax-Info Service[79].

Viele weitere Initiativen haben sich dem Kampf gegen Falschinformationen im Netz verschrieben. Vereinzelt werden auch Forderungen nach einer Anti-Fake-Behörde gestellt (vgl. Abwehrzentrum gegen Desinformation[80]).

5.4 REGULIERUNG

Laut einer Umfrage sind 86 Prozent der Deutschen für eine einfachere Kennzeichnungsmöglichkeit und neue Löschgesetze für Fake News im Internet.[81]

Ein entsprechender Schritt, um Hassreden, Falschnachrichten und strafbare Inhalte einzudämmen, soll mit dem Netzwerkdurchsetzungsgesetz[82] erreicht werden. Das Netzwerkdurchsetzungsgesetz verpflichtet soziale Netzwerke mit mehr als zwei

[75] First Draft Partnernetzwerk, https://de.firstdraftnews.com/.

[76] Mimikama, https://www.mimikama.at/.

[77] Wikitribune, https://www.wikitribune.com/.

[78] Torsten Kleinz, »Wikitribune« für besseren Journalismus: Jimmy Wales gründet Nachrichten-Plattform 25.04.2017, https://heise.de/-3693190.

[79] Hoax-Info-Service, TU Berlin, http://hoax-info.tubit.tu-berlin.de/hoax/.

[80] Horand Knaup, Gerald Traufetter, Innenministerium will Abwehrzentrum gegen Falschmeldungen einrichten, 23.12.2016, http://www.spiegel.de/netzwelt/netzpolitik/fake-news-bundesinnenministerium-will-abwehrzentrum-einrichten-a-1127174.html.

[81] Landesanstalt für Medien NRW, Neue LfM-Studie zu Fake News: Mehr als die Hälfte der Onlinenutzer hat Erfahrung damit, 19.6.2017, http://www.lfm-nrw.de/service/pressemitteilungen/pressemitteilungen-2017/2017/juni/neue-lfm-studie-zu-fake-news-mehr-als-die-haelfte-der-onlinenutzer-hat-erfahrung-damit.html.

[82] Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken, 1.9.2017, https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/DE/NetzDG.html.

Mit Taschenlampe zu erleben: Das Labyrinth Deutsche Einheit im Lügenmuseum.

Millionen registrierten Nutzern in Deutschland, wie beispielsweise Facebook, Twitter und Youtube, offensichtlich rechtswidrige Inhalte innerhalb von 24 Stunden nach Eingang einer Beschwerde zu löschen bzw. zu sperren, nicht offensichtliche nach spätestens 7 Tagen. Ansonsten drohen Strafen bis zu 50 Millionen Euro. Das Gesetz trat am 1.10.2017 in Kraft. E-Mail- und Messenger-Dienste sind von der Regulierung nicht betroffen. Kritisiert wird, dass die Unternehmen beurteilen müssen, was offensichtlich strafrechtlich relevant ist und was nicht. Daher können Löschfristen und Strafhöhe zu Überreaktionen der betroffenen Unternehmen führen, sodass im Zweifel lieber gelöscht wird, was wiederum der Meinungsfreiheit schaden kann.

Dagegen setzt die Europäische Union seit 2016 mit dem »Verhaltenskodex für die Bekämpfung illegaler Hassreden im Internet«[83] auf Selbstregulierung. Die beteiligten IT-Unternehmen (Facebook, Microsoft, Twitter und YouTube) verpflichten sich, diesbezügliche gültige[84] Meldungen in weniger als 24 Stunden zu prüfen und den Zugang zu solchen Inhalten gegebenenfalls zu entfernen oder zu deaktivieren. Auch hier liegt die Entscheidung über die Rechtmäßigkeit von Inhalten und den Umgang damit bei den Unternehmen.

[83] Europäische Kommission, http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=54300.

[84] Eine gültige Meldung sollte ausreichend genau und ausreichend begründet sein.

5.5 MEDIENKOMPETENZ

Das gesellschaftliche Problem, dass Gerüchte oder Lügen verbreitet werden, erreicht durch die enorme Reichweite digitaler Medien eine neue Dimension. Dass diesen geglaubt wird, ist häufig unabhängig vom Bildungsgrad. Die Forderung nach mehr Medienkompetenz bedeutet, dass grundlegende journalistische Kompetenzen als Allgemeinbildung gelehrt werden müssen. Gerade im Digitalen kann man sich nicht auf herkömmliche Muster und Kenntnisse verlassen. Eine korrekte Online-Recherche, Verifikation von Quellen, das Zwei-Quellen-Prinzip, sowie die Unterschiede zwischen Blogs, Kommentaren und Berichten sollten besser verstanden werden.[85]

[85] Dennis Horn, Wir brauchen eine Anti-Fake-Behörde – und andere Ideen gegen problematische Inhalte, 28.1.2016, https://blog.wdr.de/digitalistan/facebook-kommentar-fake-faelschung-geruecht/.

6. HANDLUNGSEMPFEHLUNGEN

Glaubwürdigkeit braucht Überprüfbarkeit. Unparteiische Dritte etablieren.
Der Empfänger von Informationen, Produkten, Dokumenten etc. entscheidet über deren Glaubwürdigkeit und benötigt daher Unterstützung für deren Überprüfung und Beurteilung. Neutrale, leicht auffindbare Instanzen werden benötigt, bei denen man aktuelle Informationen finden oder die Überprüfung durchführen kann. Unparteiische Dritte müssen Kontrollfunktionen auch bei vertraulichen Daten oder Algorithmen ausüben dürfen, beispielsweise hinsichtlich der Einhaltung von Selbstverpflichtungen, Kodizes, Regelungen oder Gesetzen. Da Glaubwürdigkeit nicht statisch und einmalig festzulegen ist, sollten diese Dritten auch entsprechend agieren können, Veränderungen stetig kontrollieren und dynamische Prüfungen durchführen.

Informationen einfach klassifizieren und bewerten können.
Der Übergang zwischen irreführender Darstellung und Fake ist fließend und eine Klassifizierung und Bewertung ist daher häufig komplex. Ob Fälschung, Falschbehauptung oder gar Rechtsverletzung kann in einfachen Fällen zwar maschinell markiert werden (beispielsweise manipulierte Bilder), muss in komplizierten Fällen jedoch durch Menschen (beispielsweise vom Nutzer, von einem Dienstleister oder von einem Gremium) bewertet werden. Algorithmen können diese Bewertung unterstützen.

Menschliche und algorithmische Bewertungen dürfen die freie Meinungsäußerung nicht behindern.
Nicht jede Falschnachricht soll andere beeinflussen. Wenn Nachrichten durch Menschen oder Algorithmen beurteilt werden, müssen freie Meinungsäußerung sowie Satire, Comedy oder auch Werbung von Falschnachrichten mit negativer Absicht unterschieden werden. Hetze, Verleumdung und Beleidigung müssen verfolgt werden (können). Anonymität und Verschlüsselung allein dürfen aber nicht zu einer negativen Bewertung führen.

Glaubwürdigkeit erfordert Sicherheit. Den Schutz gegen Manipulationen stetig verbessern.
Daten und Informationen, Identitäten, Algorithmen, Siegel und Zertifikate, ebenso Produkte und Produktketten müssen gegen Manipulation geschützt werden. Nur dann können diese – jedes auf seine Art – so funktionieren, wie es intendiert ist, und infolgedessen glaubwürdig sein. Schutz gegen Manipulationen wird durch Informationssicherheit (Security) und funktionale Sicherheit (Safety) der zugrundeliegenden Systeme erreicht. Beides gilt es, für die verschiedenen Zielobjekte geeignet einzusetzen und weiterzuentwickeln.

Ergebnisse künstlicher Intelligenz müssen objektiv dargestellt, geprüft, bewertet und in manchen Fällen revidiert werden können.
Intelligente Systeme unterstützen zunehmend unsere Umgebung und unser Handeln durch Empfehlungen, Ratschläge, Prognosen, Entscheidungsunterstützung oder autonome Aktivitäten. Ob diese Automatismen glaubwürdig sind, kann man als Mensch häufig nicht mehr beurteilen. Maschinelles Lernen führt zu neuen Herausforderungen. Eine objektive Darstellung, Prüfung und Bewertung algorithmischer Entscheidungen muss ermöglicht und gegebenenfalls durch Regulierung beeinflusst werden.

Medienkompetenz bereits in den Schulen lehren.
Die Beurteilung und Überprüfung des Wahrheitsgehaltes von digitalen Informationen erfordert kritischen Sachverstand, der frühzeitig und umfassend vermittelt werden muss.

GEFÖRDERT VOM

Bundesministerium
des Innern

Fraunhofer
FOKUS

Mit Taschenlampe zu erleben: Das Labyrinth Deutsche Einheit im Lügenmuseum in Radebeul-Serkowitz

KONTAKT

Petra Hoepner
Kompetenzzentrum Öffentliche IT (ÖFIT)
Tel.: +49 30 3463-7173
Fax: +49 30 3463-99-7173
info@oeffentliche-it.de

Fraunhofer-Institut für
Offene Kommunikationssysteme FOKUS
Kaiserin-Augusta-Allee 31
10589 Berlin

www.fokus.fraunhofer.de
www.oeffentliche-it.de
Twitter: @OeffentlicheIT

ISBN: 978-3-9818892-1-5

kre | 1710 (Fotos: André Wirsig)