Thematischer Beitrag

DIE DESINFORMATION

Das Wahre vom Falschen im digitalen Zeitalter unterscheiden

Vorwort

Desinformation kann viele Gesichter haben: Sie tritt als News-Artikel, User-Post, E-Mail, in Bildform oder unter der Form von *Deep Fakes*, also manipulierten Videos, auf. Diese irreführenden Informationen haben vor allem politische Folgen, indem sie sich auf demokratische Prozesse auswirken, aber auch im sozialen Bereich können sie Schaden anrichten oder sogar die eigene Gesundheit gefährden.

Heutzutage können Desinformationen so schnell verbreitet werden wie nie zuvor. Soziale Netzwerke und private Messenger bieten die Möglichkeit, falsche Informationen – die automatisiert und durch Künstliche Intelligenz (KI) gestützt sein können und dabei täuschend echt aussehen – in großem Umfang zu teilen.

Wie aber erkennt man, ob man nun wahre Informationen oder Desinformationen vorliegen hat? Und was kann man dagegen tun? Aufgrund der zunehmenden Aktualität des Themas und der sich stets verbessernden Möglichkeiten zum Generieren und Verbreiten von Desinformationen, nehmen sich bereits seit einigen Jahren staatliche Instanzen, Forschungseinrichtungen und sogar die EU an. Zahlreiche Kampagnen sollen die Menschen informieren und sensibilisieren.

Als Nutzer hat man ebenfalls Möglichkeiten, sich vor irreführenden Informationen im Internet zu schützen. In diesem Beitrag möchten wir Ihnen diese Möglichkeiten aufzeigen und Fragen rund um das Thema „Desinformation“ beantworten.

Inhaltsverzeichnis

1. Was ist Desinformation?

Der uneingeschränkte Zugang zu einer großen Anzahl an Informationen ist Grundlage für die Bildung der eigenen Meinung, insbesondere zu politischen Fragen. Das ist wichtig, um sich aktiv an öffentlichen Debatten beteiligen und den eigenen Willen in freien und fairen demokratischen Prozessen äußern zu können. Desinformationen werden gezielt verbreitet, um die Meinung der Personen innerhalb einer Gesellschaft zu beeinflussen, beispielsweise indem sie Vorurteile, Konflikte und Ängste verstärken.

Aufgefallen ist das besonders bei der US-Präsidentschaftswahl und dem Brexit-Referendum im Jahr 2016: Die mutwillige Verbreitung von Desinformationen in sozialen Medien wurde im Nachhinein als großer Einflussfaktor für die Wahl- und Abstimmungsergebnisse ermittelt. Der Begriff „Fake News" wurde für die falschen Nachrichten, die aus politischen oder finanziellen Motiven verbreitet wurden, schnell populär. Mittlerweile werden allerdings auch allgemein Falschmeldungen ohne diese Absichten als *Fake News* bezeichnet. Durch politische Instrumentalisierung etwa, indem ein politischer Akteur die Gegenmeinungen in der Öffentlichkeit als *Fake News* abtat, wurde der Begriff zusätzlich zu einem politischen Kampfbegriff. Ähnlich, wenn auch nicht ganz so verbreitet, verhält es sich mit der synonym verwendeten Bezeichnung *Hoax*.

Eine EU-Expertengruppe hat daher den Begriff „Desinformation" etabliert, der eindeutig ist und auch in der Fachsprache verwendet wird:

„Desinformation sind 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.[1]"

Desinformationen werden also **bewusst veröffentlicht, mit dem Ziel, bestimmten Personen, sozialen Gruppen, Organisationen oder Ländern zu schaden**.

Wichtig bei der Definition der Desinformation ist die **Abgrenzung zwischen Tatsachen und Meinungen**. Desinformationen enthalten immer Tatsachenbehauptungen, keine subjektiven Einstellungen oder Urteile. Damit sind sie als falsch überprüfbar. Meinungen hingegen sind persönlich, vielfältig und sollten in einer Demokratie frei zu äußern sein. Sie können auf falschen Informationen basieren, sind als Meinung aber nicht als „falsch" zu betrachten und können demnach auch nicht überprüft werden.

Ein Beispiel:

Falsche Tatsachenbehauptung: „Die Stimmabgabe bei der EU-Wahl ist strafbar, wie ein Urteil des Bundesverfassungsgerichtes beweist."

Meinung: „Die Stimmabgabe bei der EU-Wahl sollte strafbar sein."

Meinung, basierend auf falschen Tatsachen: „Ich finde es gut, dass die Stimmabgabe bei der EU-Wahl strafbar ist."

Desinformation vs. Misinformation

Desinformationen sind immer faktisch inkorrekt und es steht eine (schädliche) Absicht dahinter, die ein bestimmtes Ziel verfolgen.
Letzteres unterscheidet sie von der Misinformation, die ohne Täuschungsabsicht verbreitet wird und zum Beispiel als satirische Inhalte oder versehentliche Falschmeldungen auftritt.

2. Warum werden Desinformationen verbreitet?

Um die Beweggründe für das Verbreiten von Desinformationen zu verstehen, lohnt es sich, die Akteure genauer zu betrachten. Es gab in der Vergangenheit beispielsweise staatlich geförderte Desinformationskampagnen, wie im Bericht von 2017 vom *Europarat* festgehalten. Allerdings sind auch viele inoffizielle Akteure aktiv, darunter Gruppen oder Interessengemeinschaften, die spezifische Themen unterstützen.

Dabei sind sowohl individuelle Personen tätig wie auch durchorganisierte Gruppen. Am Prozess des Entwickelns, des Produzierens und des Verbreitens können jeweils unterschiedliche Personen und sogar **automatisierte Technologien** (*Bots*) beteiligt sein.

[1] Europäische Kommission. Aktionsplan gegen Desinformation. S.1
https://www.eeas.europa.eu/sites/default/files/aktionsplan_gegen_desinformation.pdf

Der *Europarat* nennt vier typische Motivationen für das Verbreiten von Desinformationen: finanzielle, politische, soziale und psychologische. **Sozial motiviert** ist das Teilen von Desinformationen, um sich mit anderen Unterstützern oder Gruppen zu verbinden. **Psychologische Beweggründe** sind, Ansehen oder Zuspruch zu erhalten. Am häufigsten sind allerdings die **finanziell** und **politisch** motivierten Desinformationen. Hier lohnt es sich, etwas genauer darauf einzugehen.

Finanzielle Motivation

Im Internet bringen Klicks oft Geld. Das hängt damit zusammen, dass Webseitenbetreiber mit Werbung, die auf der Seite angezeigt wird, Geld verdienen. Umso mehr Besucher eine Webseite hat (*traffic*), umso attraktiver ist sie für Werbeanzeigen, umso mehr Geld kann mit diesen verdient werden. Damit eine Webseite von vielen Usern besucht wird, werden häufig reißerische Überschriften verwendet, damit sie aufgerufen wird (sogenanntes *Clickbaiting*), wie zum Beispiel „Jeder der Wählen geht leistet Beihilfe zu einer Straftat!". Die Informationen, die man dort zu lesen bekommt, entsprechen selten der Wahrheit. Mittlerweile gibt es falsche Informations- und News-Webseiten, die komplett automatisch mit Künstlicher Intelligenz (KI) generiert werden. Werden die Inhalte hingegen von Menschen erstellt, können sogenannte „Trollfarmen" dahinterstecken, bei denen Angestellte gegen eine geringe Bezahlung diese Meldungen verfassen. Die Verbreitung der Webseiten erfolgt oftmals über soziale Netzwerke und kann sich dort selbstständig und unkontrolliert durch (unwissende) User fortsetzen. So stellt das Teilen von Desinformationen ein wenig aufwendiges, lukratives Geschäft dar.

Politische Motivation

Desinformationen, die politische Themen aufgreifen, haben oftmals zum Ziel, die Meinung der Bevölkerung zu beeinflussen. So können sie auf Wahlen Einfluss nehmen und damit auch auf politische Machtverhältnisse einwirken.

Im Rahmen der EU-Wahlen 2024 hat sich in Frankreich gezeigt, wie auf Social Media mit Hilfe von *Deep Fakes* versucht wurde, ein bestimmtes Publikum von einer parteilichen politischen Ausrichtung zu überzeugen. Die gezeigten Videos waren nicht echt, auch wenn sie so aussahen. Es handelte sich um *Deep Fakes*, bei denen die Gesichter im ursprünglichen Video durch die der Zielpersonen ersetzt wurden. So entstand der Eindruck, diese Personen würden für eine bestimmte Partei oder eine politische Ausrichtung, hier die des *Rassemblement National* (RN), werben (*Face Swap*). Ansprechend gestaltet zielten diese Videos darauf ab, die Sympathie junger Wahlberechtigter für die Partei des RN zu steigern. Hier kann man davon ausgehen, dass das Erstellen und Verbreiten dieser Desinformationen von rechtsgerichteten politischen Interessensgruppen gelenkt wurde. Desinformation in diesem Zusammenhang widmete sich auch BEE SECURE mit einem Beitrag.

3. Wo und wie werden Desinformationen verbreitet?

Heute gehören soziale Medien und Messenger-Dienste für den Großteil der Bevölkerung zum Alltag. Viele informieren sich dort tagtäglich über das Weltgeschehen und andere Dinge, die sie interessieren. Dadurch bieten diese Plattformen eine **günstige und einfache Möglichkeit, Desinformationen rasend schnell an zahlreiche Personen zu verbreiten.**

Im Vergleich zu den klassischen Medien wie Zeitung und Rundfunk ist in den sozialen Netzwerken die Sender-Empfänger-Struktur komplett anders: **Jeder Nutzer kann beide Rollen einnehmen und damit Inhalte nicht nur lesen (als Empfänger), sondern auch selbst erstellen, veröffentlichen und verbreiten (als Sender)**. Gleichzeitig findet dort meistens keine Prüfung dieser Inhalte vor der Veröffentlichung statt.

So kann jeder wissentlich oder unwissentlich zur Weitergabe von Desinformation beitragen.

Nehmen wir das Beispiel des *Deep-Fake*-Videos der vermeintlichen Politikerin und ihrer Nichte, um die Verbreitungswege zu verdeutlichen: Ein Parteianhänger erstellt das Video mit einem *Face-Swap*-Programm und postet es als Fake-Profil auf *TikTok* (als Produzent und Sender), um der Partei ein attraktives Image zu verleihen und junge Menschen zu motivieren, sie zu wählen. User, die das Video sehen (als Empfänger), teilen es beispielsweise auf *Facebook* oder über *Messenger* wie *Telegram* (als Sender), entweder, weil sie die Botschaft unterstützen oder um ihren *Followern* (die Leute, mit denen sie vernetzt sind) ihre Ablehnung zu zeigen. In beiden Fällen hat der ursprüngliche Produzent des Videos erreicht, was er wollte: Das Video und die Desinformation werden verbreitet.

Zusätzlich wird die Verbreitung von personalisierten Algorithmen beeinflusst.

Algorithmen und Filterblasen

In sozialen Netzwerken hat jeder seine „eigene Sicht auf die Welt". Welche Posts Sie zu sehen bekommen, hängt von einem **Personalisierungsalgorithmus** ab. **Dieser sammelt Informationen darüber**, wonach Sie im Internet gesucht haben, was Sie angesehen, ***geliked***, geschrieben und gekauft haben. Damit wird sichergestellt, **dass Ihnen vorwiegend Inhalte angezeigt werden, die Ihre Vorlieben und Sichtweise treffen**. Sie befinden sich in Ihrer „Filterblase" (engl. ***filter bubble***), in die es andere Inhalte nur schwer hineinschaffen.

Problematisch daran ist, dass Themen oft nur aus einer Perspektive wahrgenommen werden und diese einseitige Sicht verstärkt wird, insbesondere, je öfter man eine bestimmte Information liest („illusorischer Wahrheitseffekt", engl. *truth effect*). Falsche Informationen werden leichter geglaubt, wenn sie sich in das eigene Weltbild einfügen und die eigene Meinung stützen (*confirmation bias*).

Und auch Produzenten von Desinformation wissen, wie sie die Algorithmen nutzen können, indem sie mit gezielten Schlagworten versuchen, in häufig vorkommende *Bubbles* reinzukommen.

Desinformationen im Internet sind, was ihre Verbreitung angeht, darauf angewiesen, dass sie von den Nutzern der sozialen Netzwerke geteilt werden. Das Erstellen wiederum kann manuell durch einzelne Nutzer, durch Trollfarmen, aber auch (halb-)automatisiert erfolgen.

Für Letzteres werden sogenannte ***Social Bots*** verwendet. Dabei handelt es sich um Fake-Profile in sozialen Netzwerken, die aussehen und sich verhalten wie echte Menschen, aber von einem Programm gesteuert werden. Sie können posten, liken und kommentieren. Oftmals basieren Sie auf sogenannten KI-Sprachmodellen (Algorithmen, die Sprache verarbeiten, „verstehen" und erzeugen können), weswegen ihre Antworten noch vielfältiger und natürlicher wirken können.

Dazu lernen diese KI-Modelle anhand von Posts aus öffentlichen Social-Media-Kanälen, die eine bestimmte Meinung vertreten oder ein ausgewähltes Thema behandeln, diese Meinungen in selbst erzeugten Texten wiederzugeben. Sie werden eigentlich im Marketing verwendet, um in den Dialog mit (potentiellen) Kunden zu treten und für bestimmte Dinge zu werben. Aber auch für meinungsbildende Zwecke in der Politik können sie genutzt werden, was sie gefährlich macht: So können sie zum Beispiel in großem Stil Aussagen für eine politische Partei erzeugen und die Gegenpartei „schlechtreden".

Social Bot?

Zu erkennen ist ein ***Social Bot*** zumeist daran, **dass der Account sehr viele Posts in kurzer Zeit produziert** – schließlich sollen damit viele einschlägige Informationen in kurzer Zeit generiert werden. Auch, wenn man mit ihm direkt kommuniziert, **antwortet er meist innerhalb von Sekunden. Bei Fragen außerhalb seines eigentlichen Themas versagt er oftmals**. Im Gegensatz zu echten Accounts wird **ein *Social Bot* niemals einen blauen Haken im Profil haben** – dieser zeigt in vielen Netzwerken an, dass es sich um einen verifizierten, echten Account handelt. **Der Blick ins Profil lohnt sich auch sonst: Oftmals haben *Social Bots* nur sehr generelle oder keine Informationen drinstehen**, der Nickname enthält manchmal wirre Zahlen- und Buchstabenketten und das Foto fehlt ganz oder ist generisch.

Die gleiche Technologie kann zum Erstellen von falschen News-Webseiten genutzt werden. Dann werden statt Postings Nachrichtenartikel für das KI-Modell verwendet (sogenanntes ***Content Farming***). Hier stehen meist finanzielle Intentionen im Vordergrund, weshalb diese Seiten viel Werbung enthalten. Enttarnen kann man sie oftmals durch fehlende Urheber- und Autorenangaben. Zudem können die Texte unplausibel wirken und dem allgemeinem Weltwissen widersprechen.

4. Welche Gefahr kann von Desinformationen ausgehen?

Die schädlichen Auswirkungen von Desinformationen können sowohl Sie persönlich treffen als auch die gesamte Öffentlichkeit. Damit ist gemeint, dass sie in die Politik, in demokratische Prozesse wie beispielsweise Wahlen, eingreifen, aber auch die Sicherheit und Umwelt beeinflussen können. Nicht zuletzt kann sogar die eigene Gesundheit darunter leiden.

So kann das konkret aussehen:

- **Demokratie:** Eine mit einem Gerichtsurteil untermauerte Information zur Europawahl 2024, „Jeder der Wählen geht leistet Beihilfe zu einer Straftat“, sollte Politikverdrossenheit schaffen. Das bereits in Kapitel 2 erwähnte *Deep-Fake*-Video dient zum Wählerfang für eine rechtspopulistische Partei. Sowohl das Brexit-Referendum wie auch die US-Präsidentschaftswahlen 2016 wurden nachweislich durch staatliche Desinformationskampagnen beeinflusst.
- **Sicherheit:** Dem Ukraine-Krieg ging eine jahrelange, gut organisierte russische Desinfomationskampagne des Kremls voraus. In beiden Ländern wurden gezielt Desinformationen verbreitet, um die Ukraine zu schwächen, zu destabilisieren und als Feind zu deklarieren. Damit sollte der Angriff auf die Ukraine legitimiert werden.
- **Gesundheit:** Während der Covid-19-Pandemie schürten viele Beiträge in den sozialen Medien Unsicherheit über die Behandlung, die Sicherheit und Wirksamkeit der Impfstoffe, den Nutzen der sozialen Distanzierung und vieles mehr. Dies führte zu sozialen Protesten und Unruhen, zusätzlich erlebten viele persönliche Konflikte und Ausgrenzungen im eigenen Arbeits- und sozialen Umfeld. Die Impfstoffe wurden nicht so schnell angenommen wie nötig. In einigen Fällen gab es sogar mehr Tote. Ein aktuelleres Beispiel bilden „Pilzratgeber“, die auf Amazon erworben werden konnten. Diese sind KI-generiert, die Informationen nicht auf ihre Richtigkeit überprüft. Essbare Pilze sehen oft giftigen Arten sehr ähnlich, weshalb selbst kleine Fehler, wie sie bei KIs vorkommen können, in diesem Fall lebensgefährlich sein können.
- **Im persönlichen Umfeld** können Desinformationen ebenfalls großen Schaden anrichten, indem sie gezielt für Mobbing und Erpressungen genutzt werden. Beispielsweise können mit *Deep-Fake-Porn* und *Face-Swap*-Anwendungen pornografische Inhalte mit den Gesichtern gewünschter Personen erzeugt und für Mobbing und Erpressungen verwendet werden.

Bei Desinformationen handelt es sich also um **Online-Gefahren, die fatale realweltliche Auswirkungen** haben können.

Eine Studie im BEE SECURE Radar 2024 zeigt, dass Desinformationen mitunter die am meisten wahrgenommenen Gefahren online sind:

- Desinformation und Fake News wurden bei den 129 befragten jungen Leuten zwischen 17 und 30 Jahren mit 50 % als das am meisten beunruhigende Online-Risiko genannt.
- Bei den 283 befragten Eltern der 12- bis 16-Jährigen werden sie auf dem zweiten Platz mit 42 % genannt;
- Die 217 befragten Eltern der 3- bis 11-Jährigen haben die Gefahr mit 25 % geringer eingeschätzt.

5. Der Kampf gegen Desinformation

Um der wachsenden Bedrohung, die von Desinformationen ausgeht, entgegenzutreten, ergreifen Regierungen und Organisationen weltweit Maßnahmen, die die Bevölkerung und die politische Öffentlichkeit davor schützen sollen. Dabei ist die Zusammenarbeit über die Grenzen hinaus wichtig, um Informationen auszutauschen und gemeinsame Strategien zu entwickeln.

- **Stärkere Zusammenarbeit**
  Die *Europäische Union* hat mehrere Initiativen entwickelt, darunter den Aktionsplan gegen Desinformation 2018 und den Europäischen Aktionsplan für Demokratie 2020. Diese Pläne stärken die Zusammenarbeit und Transparenz in der EU. Seit 2019 tauschen europäische Institutionen und die EU-Mitgliedstaaten mit einem „Frühwarnsystem" schnell Informationen und etwaige Auffälligkeiten aus. Mit der Unterzeichnung der *Global Declaration on Information Integrity Online* haben sich über dreißig Staaten auf der ganzen Welt zusammengetan, um mit verschiedenen Strategien gegen Desinformation vorzugehen.
- **Bessere Erkennung und Analyse von Desinformationen**
  Es wird mehr Geld in Daten- und Faktenüberprüfung, Forschung und geschultes Personal investiert. Die Europäische Beobachtungsstelle für digitale Medien (*European Digital Media Observatory, EDMO*), eine unabhängige Beobachtungsstelle, unterstützt die Faktenchecker und Forscher im Bereich Desinformation und überwacht die Anwendung von Strategien gegen Desinformation. Ein weiteres Beispiel ist die East *StratCom* Task Force des Europäischen auswärtigen Dienstes, die sich mit dem Projekt *EUvsDisinfo* auf das Aufdecken und Vereiteln russischer Desinformationskampagnen spezialisiert hat.
- **Große Akteure auf dem digitalen Markt regulieren und überprüfen**
  2018 wurde der EU-Verhaltenskodex zur Desinformation erlassen und 2022 noch einmal verschärft. Zahlreiche große Firmen, wie *Google*, *Microsoft*, Meta und *TikTok* haben sich (freiwillig) verpflichtet, ihn einzuhalten. Damit gewährleisten sie mehr Transparenz und verpflichten sich, gegen illegale Inhalte und Desinformation verstärkt vorzugehen. Verstöße werden von der *EU-Kommission* überprüft und geahndet.
- **Illegale Inhalte einfacher entfernen und Werbung besser kennzeichnen**
  Seit 2024 ist der 2022 in Kraft getretene *Digital Services Act* (DSA) vollumfänglich gültig. Er soll innerhalb der gesamten EU den digitalen Raum sicherer gestalten und dabei Nutzer-Grundrechte wie die Redefreiheit sichern. Das betrifft alle digitalen Dienste, die Verbrauchern Waren, Dienstleistungen oder Inhalte anbieten, auch wenn sie sich außerhalb der EU befinden. Damit sind Social-Media-Plattformen, aber auch Hosting-Dienste und Online-Märkte gemeint. Digitale Dienste müssen nun schneller gegen illegale und missbräuchliche Inhalte, wie zum Beispiel *Social Bots* oder Hassrede (*Hate Speech*), vorgehen und die Transparenz weiter steigern.
- **Zuverlässigere Informationen bereitstellen und stärker über Desinformation informieren**
  Unabhängige Medien und Faktenchecker werden mehr unterstützt. Ein Beispiel ist das *European Fact-Checking Standards Network*. Es besteht aus mehreren europäischen Faktencheckerorganisationen. Es legt Standards für *Fact-Checking* fest, bildet Faktenchecker aus und klärt bei spezifischen Themen wie der Klimakrise und der *Europawahl 2024* über konkrete Fälle von Desinformation auf.

- **Die Gesellschaft sensibilisieren und widerstandsfähiger gegen Desinformationen machen**
  Menschen in Europa und darüber hinaus werden über Risiken informiert und ihnen wird gezeigt, wie sie Desinformationen erkennen und bekämpfen können. Dazu gibt es zahlreiche Kampagnen, die schon bei den Kleinsten ansetzen: Mit der *Better Internet for Kids Initiative* (BIK) in Zusammenarbeit mit dem von der EU kofinanzierten Netz von Safer-Internet-Zentren in den Mitgliedstaaten (davon BEE SECURE als Vertreter von Luxemburg) will die EU Online-Plattformen für Kinder sicherer machen und gleichzeitig die Medienkompetenz von Kindern schulen. Sie stellt Informationen für Kinder, ihre Eltern, Lehrende, aber auch für Forschung und Industrie bereit.

  Der *Digital Education Action Plan (2021–2027)* der EU richtet sich an alle Zielgruppen: Er legt fest, wie man die Medienkompetenz von allen EU-Bürgern verbessern kann, etwa in Schulen oder mit kostenlosen digitalen Workshops (zum Beispiel über den *European Digital Education Hub*).

  In Luxemburg sensibilisiert BEE SECURE die breite Öffentlichkeit für einen sicherheitsorientierten und verantwortungsvollen Umgang mit digitaler Technologie. Insbesondere für Kinder, Jugendliche und deren Umfeld (Eltern, Lehrer, Erzieher und andere) gibt es vielseitige Angebote und Aktivitäten rund um eine sichere Internetnutzung. Sensibilisierungstrainings bilden dabei den Schwerpunkt. Ebenso wie die vielfältigen Publikationen decken auch die Trainings ein breites Themenspektrum ab. Darüber hinaus führt die Initiative regelmäßig thematische Kampagnen und Veranstaltungen durch.

  Im Rahmen dieser Bemühungen wird das Thema der Desinformation regelmäßig – auch in Zusammenarbeit mit Partnern wie u. a. dem *Zentrum fir politesch Bildung, ALIA und EDMO Belux* – beleuchtet. Außerdem ist Medienbildung als *Digital Sciences* bereits ins Schulprogramm integriert.

6. Was kann ich gegen Desinformation tun?

Desinformationen haben zahlreiche Ausprägungen – Text, Bild, Video, Audio. Sie können Ihnen überall im Internet begegnen, beispielsweise als Posts in sozialen Netzwerken, in Ihrem E-Mail-Postfach, als *Reel* (Kurzvideo) auf *Instagram*, als *Whatsapp*-Nachricht und an vielen anderen Orten. Schutzlos ausgeliefert sind Sie Ihnen aber nicht!

Eine gute Methode, um bereits gewappnet zu sein, ist das sogenannte ***Prebunking***: Umso mehr Sie schon vorweg über Desinformationen und entsprechende Strategien wissen, umso eher erkennen Sie sie.

Prebunking

Prebunking meint das präventive Aufklären über Desinformation und ihre Mechanismen. Insbesondere in politischen Kontexten ist es oftmals schwierig, im Nachhinein durch Methoden wie Faktenchecking bzw. Debunking eine Desinformation wieder verschwinden zu lassen. Häufig hat sie bereits Auswirkungen während ihrer Verbreitung und nur ein kleiner Anteil der Empfänger ist danach noch für eine Korrektur erreichbar.

Eine europaweite Prebunking-Kampagne von der Google-Tochter *Jigsaw* und verschiedenen Organisationen informiert Sie über gängige Manipulationsstrategien. Wenn Sie diese kennen, können Sie sie leichter enttarnen!

Drei sehr verbreitete Desinformationsmechanismen sollen hier als Beispiel kurz vorgestellt werden. Über die jeweilige Verlinkung können Sie sich das Kampagnenvideo dazu anschauen:

1. **Die Sündenbock-Methode:**
   Bei der Sündenbock-Methode wird eine bestimmte Person oder eine Personengruppe fälschlicherweise allein für ein Problem verantwortlich gemacht. Solche Anschuldigungen sollten immer auf ihre Richtigkeit geprüft werden.

2. **Dekontextualisierung:**
   Bei der Dekontextualisierung werden Videos und Bilder im falschen Kontext verwendet oder durch KI generiert oder verändert. Auch fehlen vertrauenswürdige Quellen zu den veröffentlichten Informationen, die oftmals besonders überraschend oder schockierend sind.
3. **Rufschädigung:**
   Bei der Rufschädigung werden Aussagen über Personen oder Personengruppen getätigt, die ihren Charakter und ihre Glaubwürdigkeit in Frage stellen. Beweise dafürsucht man vergebens.

Natürlich gibt es noch weitere Manipulationsstrategien, wie etwa emotionale Sprache, falsche Experten oder inkohärente Argumentationen. Eine leicht verständliche Übersicht bietet die Kampagnenwebseite.

Für den konkreten Fall hat BEE SECURE eine **Checkliste** erstellt, **mit der Sie Informationen auf Ihre Echtheit prüfen können**. Damit können Sie sich schützen und zusätzlich die Verbreitung von Desinformation verhindern.

Zwar dauern erste Überprüfungen sicher etwas, aber „Übung macht den Meister!". Mit der Zeit werden Sie sicherer und schneller, sodass Sie die Checkliste irgendwann nicht mehr benötigen.

Damit die Checkliste auch in die Hosentasche bzw. auf ein Smartphone-Foto passt, finden Sie hier die kompakte Version. Eine ausführlichere Version mit weiteren Details erhalten Sie im Anhang.

1. **Wer steckt hinter den Informationen?**
   a. Wer ist der Autor? Unbekannt oder nicht vorhanden Schlechtes Zeichen!
   b. Wer hat die Information geteilt? Hat derjenige die Information überprüft?
   c. Sind Konto oder Website echt? Impressum, Profilinformationen und Postverhalten beachten.
   d. Welche Intention steckt hinter der Information? Was ist das Ziel?
2. **Vertrauenswürdige Quelle?**
   Sind Zahlen oder Fakten korrekt belegt?
   Wird auch woanders darüber berichtet?
3. **Wie berichten andere davon?**
   Querlesen und Faktenchecker fragen!
4. **Wie wird die Information dargestellt?**
   - Passen alle Bestandteile wie Überschrift, Text und Bilder inhaltlich zusammen? (Bilder-Rückwärtssuche nutzen!)
   - Ist der Text verallgemeinernd, einseitig oder nicht schlüssig?
     → Warnzeichen!
   - Tatsache oder Meinung?
   - Werden gezielt starke Emotionen ausgelöst?
     → Ebenfalls ein Warnzeichen!
5. **Check yourself !**
   - Wie tief stecken Sie in Ihrer eigenen Filterblase?

Nützliche Links

- EUnVDnDisinfo : https://euvsdisinfo.eu/de
- Prebunking : https://prebunking.withgoogle.com/de
- EDMO Fact-checking : https://belux.edmo.eu/fact-checking
- Mimikama : https://mimikama.org
- Correktiv : https://correctiv.org
- Politifact : https://politifact.com
- FactCheck : https://factcheck.org
- snopes : https://snopes.com

- European Digital Education Hub: education.ec.europa.eu/focus-topics/digital-education/action-plan/european-digital-education-hub

- Interaktiver Test zur eigenen Filterblase: www.bee-secure.lu/de/tool/interaktiver-test-zur-eigenen-filterblase

Bibliografie

- **BEE SECURE**. BEE SECURE Radar 2024 www.bee-secure.lu/de/publikation/bee-secure-radar
- **Better Internet for Kids**. The rising importance of disinformation in media literacy www.betterinternetforkids.eu/practice/articles/article?id=7225534
- **Conseil de l'Europe**. Information disorder: Toward an interdisciplinary framework for research and policy making (2017) https://edoc.coe.int/fr/medias/7495-information-disorder-toward-an-interdisciplinary-framework-for-research-and-policy-making.html
- **European Union: External Action**. Action Plan against Disinformation www.eeas.europa.eu/node/54866_en
- **EUnVDnDisinfo**. https://euvsdisinfo.eu/de
- **franceinfo**. Réseaux sociaux : l'Europe durcit le ton sur la désinformation www.francetvinfo.fr/internet/reseaux-sociaux/facebook/reseaux-sociaux-l-europe-durcit-le-ton-sur-la-desinformation_6133656.html
- **klicksafe**. Prebunking – So schützt man präventiv gegen Desinformationen www.klicksafe.de/news/prebunking-so-schuetzt-man-praeventiv-gegen-desinformationen
- **Luxemburger Wort**. Ermittlungen gegen Facebook und Instagram www.wort.lu/wirtschaft/ermittlungen-gegen-facebook-und-instagram/12391748.html
- **JIGSAW l Google**. Prebunking https://prebunking.withgoogle.com/de
- **toute l'europe**. Désinformation : la Commission européenne ouvre une enquête contre le réseau social X (ex-Twitter) www.touteleurope.eu/economie-et-social/desinformation-la-commission-europeenne-ouvre-une-enquete-contre-le-reseau-social-x-ex-twitter
- **Saferinternet.at**. Was ist ein Social Bot? www.saferinternet.at/faq/informationskompetenz/was-ist-ein-social-bot
- **Saferinternet.at**. Wie erkenne ich Social Bots? www.saferinternet.at/faq/informationskompetenz/wie-erkenne-ich-social-bots
- **Saferinternet.at**. Was ist ein Algorithmus und wie entstehen Filterblase? www.saferinternet.at/was-ist-ein-algorithmus-und-wie-enstehen-filterblasen
- **The New York Times**. See How Easily A.I. Chatbots Can Be Taught to Spew Disinformation www.nytimes.com/interactive/2024/05/19/technology/biased-ai-chatbots.html
- **U.S. Department of state**. Building A More Resilient Information Environment www.state.gov/building-a-more-resilient-information-environment
- **bpb**. Fake News, Misinformation, Desinformation www.bpb.de/shop/zeitschriften/izpb/medienkompetenz-355/539986/fake-news-misinformation-desinformation
- **mimikama**. Nein, die Stimmabgabe bei den Europawahlen ist keine Straftat www.mimikama.org/stimmabgabe-eu-wahlen-2024-keine-straftat
- **BEE SECURE**. Europawahlen: Manipulation durch Desinformation mit Deepfakes www.bee-secure.lu/de/news/europawahlen-desinformation-mit-deepfakes

- **SOCIAL MEDIA PSYCHOLOGY**. The psychology of fake news: how disinformation spreads online https://socialmediapsychology.eu/2018/09/20/the-psychology-of-fake-news-how-disinformation-spreads-online
- **Online Lexikon für Psychologie & Pädagogik.** confirmation bias https://lexikon.stangl.eu/10640/confirmation-bias-bestaetigungsfehler-bestaetigungstendenz#google_vignette
- **EuvsDisinfo**. „Gegen die fortlaufenden Desinformationskampagnen von Russland vorgehen“: acht Jahre EUvsDisinfo https://euvsdisinfo.eu/de/gegen-die-fortlaufenden-desinformationskampagnen-von-russland-vorgehen-acht-jahre-euvsdisinfo
- **World Health Organization**. Disinformation and public health www.who.int/news-room/questions-and-answers/item/disinformation-and-public-health
- **heise**. „Völlig unverantwortlich“ : KI-generierte Pilzratgeber bei Amazon angeboten www.heise.de/news/Voellig-unverantwortlich-KI-generierte-Pilzratgeber-bei-Amazon-angeboten-9293723.html
- **Europäische Kommission**. Schutz der Demokratie https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/new-push-european-democracy/protecting-democracy_de
- **European Digital Media Observatory** https://edmo.eu
- **Europäische Kommission**. Verhaltenskodex 2022 zur Bekämpfung von Desinformation https://digital-strategy.ec.europa.eu/de/policies/code-practice-disinformation
- **Europäische Kommission**. Paket zum Gesetz über digitale Dienste https://digital-strategy.ec.europa.eu/de/policies/digital-services-act-package
- **EFCSN**. Advancing fact-checking https://efcsn.com/advancing-fact-checking
- **Europäische Kommission**. Eine europäische Strategie für ein besseres Internet für Kinder (BIK+) https://digital-strategy.ec.europa.eu/de/policies/strategy-better-internet-kids
- **EUR-Lex**. Aktionsplan für digitale Bildung (2021-2027) https://eur-lex.europa.eu/DE/legal-content/summary/digital-education-action-plan-2021-2027.html
- **Europäische Kommission**. Tackling Disinformation and Information Manipulation https://ec.europa.eu/commission/presscorner/api/files/attachment/878789/Tackling Disinformation_Factsheet_DE.pdf
- **DW**. Faktencheck: Wie erkenne ich KI-generierte Websites? www.dw.com/de/faktencheck-was-sind-ki-generierte-websites-und-wie-erkenne-ich-sie/a-65546851
- **DW**. Faktencheck: Wie man Desinformation vor EU-Wahlen erkennt www.dw.com/de/faktencheck-wie-man-desinformation-im-europawahlkampf-erkennt/a-69008051
- **Le Gouvernement du Grand-Duché de Luxembourg**. digital sciences https://innovative-initiatives.public.lu/initiatives/digital-sciences

Herausgeber: Service national de la jeunesse (SNJ)
Service national de la jeunesse - B.P. 707 L-2017 Luxembourg
www.snj.lu | www.bee-secure.lu

© 2025 Service national de la jeunesse (SNJ) – Initiative BEE SECURE
Die Creative-Commons-Lizenz dieser Publikation nachlesen : www.creativecommons.org/licenses/by-nc-sa/4.0/deed.de

Thematischer Beitrag
Die Desinformation
Das Wahre vom Falschen im digitalen Zeitalter unterscheiden
11.2025
ISBN 978-2-919828-91-3
elektronische Ressource

Initiiert von: LE GOUVERNEMENT DU GRAND-DUCHÉ DE LUXEMBOURG Ministère de l'Éducation nationale, de l'Enfance et de la Jeunesse

Durchgeführt von: Service national de la jeunesse; KJT.lu

Kofinanziert von: Kofinanziert von der Europäischen Union