

Politische Microtargeting, KI und Plattformregulierung – Entwicklungen bis 2025 für "Projekt Klarblick"

Microtargeting im politischen Kontext: Datengetriebene Beeinflussung

Gezielte Ansprache von Wählenden: Microtargeting bezeichnet die hochgranulare Ausrichtung politischer Botschaften auf spezifische Personengruppen oder sogar Individuen anhand von Datenprofilen. In den letzten Jahren hat diese Methode erheblich an Präzision gewonnen, befeuert durch immer größere Datensammlungen und Künstliche Intelligenz. Bekannt wurde der Ansatz spätestens seit dem *Cambridge-Analytica*-Skandal, bei dem 2016/17 via Facebook-Daten persönliche Profile erstellt wurden, um Wähler mit zugeschnittenen Botschaften zu beeinflussen. Heute – rund acht Jahre später – sind solche personalisierten Kampagnen zwar stärker reguliert (siehe unten), aber nach wie vor weltweit im Einsatz ¹.

Neue KI-Strategien im Wahlkampf: Durch Fortschritte bei *Generative AI* können Wahlkämpfer inzwischen automatisiert Hunderte Varianten einer Botschaft erstellen, jeweils zugeschnitten auf Interessen, Emotionen oder sogar Persönlichkeitstypen ihrer Zielpersonen. Ein frühes Beispiel lieferte die US-Politik: 2023 veröffentlichte das Wahlkampfteam der Republikanischen Partei ein vollständig KI-generiertes Video als Antwort auf Präsident Bidens Bewerbung – es inszenierte eine dystopische Zukunft unter Biden und wurde komplett aus synthetisch erzeugten Bildern zusammengesetzt ². Solche KI-Medien verdeutlichen, wie schnell und kostengünstig heute politische *Attack Ads* oder *Fake News* produziert werden können. Auch in Deutschland sind erste Vorboten dieses Trends erkennbar: So sorgte kürzlich ein KI-generiertes Video des CDU-Politikers Friedrich Merz – geteilt vom SPD-Bundestagsabgeordneten Bengt Bergt – für Schlagzeilen und entfachte die Debatte über den KI-Einsatz im Wahlkampf ³. Diese Beispiele zeigen, dass Microtargeting längst nicht mehr nur statische Facebook-Anzeigen bedeutet, sondern dynamische KI-Inhalte umfasst, die in sozialen Netzwerken oder Messengern hochpersonalisiert ausgespielt werden können.

Personalisierte Desinformation: Die Kehrseite von präzisiertem Targeting ist das Risiko, dass Falschinformationen passgenau verbreitet werden. In Ländern wie Indien etwa wurde deutlich, wie einfach Wählerdaten für **personalisierten Fake Content** genutzt werden können ⁴. Die regierende BJP setzte dort eine App namens *Saral* ein, um Millionen von Bürgerdaten auf Mikro-Ebene zu sammeln – darunter Alter, Geschlecht, Religion, Kaste und Adresse – und bezeichnete sie intern als „**wahlentscheidende Maschine**“ ⁴ ⁵. Auf Basis solcher Profile lassen sich Gerüchte oder Verschwörungstheorien gezielt an empfängliche Bevölkerungssegmente senden, während andere Gruppen andere Botschaften sehen. Das Ergebnis ist eine fragmentierte *Filterblase*: Jede Gruppe bekommt ihre „eigene Wahrheit“ serviert. Beobachter warnen, dass diese **digitalen Echokammern** die gesellschaftliche Spaltung vertiefen und Wähler unbemerkt manipulieren können. Insbesondere **personalisiertes Lügenmaterial** – etwa irreführende Wahlkampfbehauptungen, die genau an bestehende Ängste oder Vorurteile einzelner Zielpersonen anknüpfen – gilt als demokratiegefährdend

Debatte um Eindämmung: Angesichts dieser Gefahren ist international eine rege Debatte entbrannt, ob Microtargeting in der politischen Werbung eingeschränkt oder gar verboten werden sollte. Demokratie-Aktivist*innen führen ins Feld, dass *undurchsichtige Datenprofile* und geheime Werbeanzeigen die Gleichheit der Wahl untergraben. Selbst Big-Tech-Unternehmen haben auf öffentlichen Druck reagiert: Google etwa schreibt seit Ende 2023 vor, dass politisch geschaltete Anzeigen deutlich kennzeichnen müssen, wenn sie KI-generierte Inhalte enthalten ⁶. In der EU wurde das Thema ebenfalls adressiert (siehe nächster Abschnitt zur Regulierung). Allerdings sind sich Experten uneins, wie strikt die Grenzen gezogen werden sollten – schließlich nutzen auch etablierte Parteien legale Datenanalyse, um legitime Botschaften effizienter zu platzieren. Die Diskussion bewegt sich somit zwischen *Wahlkampffreiheit* und *Wählerschutz*. Klar ist jedoch: Microtargeting bleibt 2025 ein zentrales Schlagwort, wenn es um moderne **Wahlkampfstrategien** geht, und liefert reichlich realen Stoff für das fiktionale Szenario von „Projekt Klarblick“.

Algorithmen- und Plattformregulierung: DSA, DSA und neue Gesetze

Digital Services Act (DSA) – neuer Ordnungsrahmen: In Europa ist 2024 ein **Meilenstein** für die Plattformregulierung erreicht worden. Am 17. Februar 2024 trat der *Digital Services Act* vollständig in Kraft, mit dem die EU ein „Regelwerk für ein sichereres, faireres und transparenteres Internet“ geschaffen hat ⁷ ⁸. Der DSA verpflichtet Online-Plattformen dazu, **systematische Risiken** für Gesellschaft und Demokratie zu analysieren und zu minimieren – ausdrücklich genannt werden etwa manipulative Algorithmen oder die Verbreitung von Desinformation ⁹. Sehr große Plattformen (sog. VLOPs wie Facebook, YouTube, X/Twitter) müssen nun regelmäßig Berichte vorlegen und unabhängigen Prüfungen standhalten. Die EU-Kommission scheut sich nicht, Verstöße zu ahnden: Gegen Elon Musks Plattform X etwa wurden bereits Ende 2023 offizielle Verfahren eingeleitet – u.a. wegen mangelhafter Transparenz und unzureichenden Vorgehens gegen illegale Inhalte und Desinformation ⁸. Kurz nach Inkrafttreten des DSA folgte ein ähnliches Verfahren gegen TikTok bezüglich Schutz Minderjähriger und mangelnder Datenzugänge für Forschende ⁸. Diese frühen Durchsetzungen senden ein klares Signal: **Aufsichtsbehörden greifen durch**, um die Online-Welt demokratieverträglicher zu gestalten. Künftig sollen insbesondere Kinder- und Jugendschutz, Hassrede und **Wahlintegrität** im Fokus stehen ¹⁰. So hat die EU-Kommission eigens *DSA-Wahlleitlinien* und 2025 ein *Toolkit* für nationale Aufseher veröffentlicht, um bewährte Maßnahmen gegen Wahlmanipulation zu bündeln – inklusive dem Umgang mit KI-generierten Inhalten und Identitätsmissbrauch ¹¹.

Transparenz und Datenzugang: Ein zentrales Anliegen der Regulierung ist zudem, die **Black Box** der Algorithmen etwas zu lüften. Der DSA schreibt vor, dass Nutzer mehr Kontrolle über Empfehlungsalgorithmen erhalten (etwa chronologische Feeds wählen können) und dass **Werbeplattformen politische Anzeigen mit zusätzlichen Informationen versehen** müssen. So entsteht etwa in der EU eine öffentliche Anzeigen-Datenbank, in der Bürger nachschauen können, *wer* hinter einer politischen Anzeige steckt, *welches* Publikum anvisiert wurde und *wieviele* Geld geflossen ist ¹² ¹³. Dies soll der bisher oft unsichtbaren Microtargeting-Praxis zumindest im Nachhinein etwas Licht bringen. Forschenden wird überdies gemäß DSA ein Zugang zu Plattformdaten ermöglicht, um Phänomene wie Desinformationsverbreitung wissenschaftlich untersuchen zu können – ein wichtiger Schritt, den die Zivilgesellschaft lange forderte. Parallel haben die großen sozialen Netzwerke freiwillige Verhaltenskodizes gegen Desinformation unterzeichnet. Diese **Verhaltenskodizes** – zum Beispiel der *EU Code of Practice on Disinformation* – wurden Anfang 2025 offiziell in den DSA-Rahmen integriert, was bedeutet, dass konsequente Einhaltung nun als Maßstab für die DSA-Compliance der Unterzeichner dient ¹⁴. Konzerne wie Meta, Google, TikTok oder Microsoft bekennen sich damit (weiterhin) zu Maßnahmen wie dem Löschen von Fake-Accounts, der Kennzeichnung manipulativer Bots und der Zusammenarbeit mit Faktenprüfern. Wichtig: Firmen, die sich solchen Standards entziehen (wie X, das

2023 aus dem Kodex austrat), laufen Gefahr, beim nächsten Desinformationsvorfall verstärkt aufs Korn genommen zu werden – die EU kann Strafen von bis zu 6% des weltweiten Jahresumsatzes verhängen

15 .

Gezielte politische Werbung unter Aufsicht: Ergänzend zum DSA hat die EU im **März 2024** eine spezielle Verordnung für **Transparenz und Targeting politischer Werbung** beschlossen 16 . Diese schreibt vor, dass politische Anzeigen eindeutig als solche gekennzeichnet werden und eine Reihe von Informationen leicht abrufbar bereitstellen müssen – darunter wer die Anzeige finanziert, auf welche Wahl sie sich bezieht und ob **Targeting-Techniken** genutzt wurden 17 . Vor allem aber schränkt das Gesetz Mikrotargeting in der EU deutlich ein: Die Nutzung persönlicher Daten für politische Werbung **ist nur noch erlaubt, wenn die Person** vorher ausdrücklich eingewilligt **hat** 18 . Daten von Dritten (gekaufte Datenbestände) dürfen nicht mehr heimlich eingesetzt werden, und besonders sensible Merkmale – etwa Ethnie, Religion, Gesundheit **und politische Meinung** – **dürfen gar nicht mehr zur Profilbildung herangezogen werden** 18 . Damit setzt Europa auf ein Opt-in-Modell: Nutzer sollen aktiv *Ja* sagen müssen, bevor sie z.B. anhand ihres Online-Verhaltens auf Parteien zugeschnittene Botschaften erhalten. Theoretisch kann nun also jeder Bürger pauschal widersprechen, „persönliche“ Wahlwerbung zu bekommen, was einem Verbot im Einzelfall gleichkäme 19 . Allerdings bleibt abzuwarten, wie effektiv das in der Praxis ist. Kritiker monieren nämlich, dass die Regeln Schlupflöcher lassen: So dürfe weiterhin anhand allgemeiner Interessen, Nutzungsgewohnheiten oder statistischer Zwillinge zielgruppengerecht geworben werden 20 – was faktisch eine Fortsetzung der „Überwachungswerbung“ mit anderen Mitteln ermögliche 1 . Patrick Breyer, Europaabgeordneter der Piratenpartei, bezeichnete die Targeting-Regeln gar als „Farce“: *Digital manipulative Wahlwerbung im Stile Cambridge Analytics bleibt legal*, solange nicht direkt verbotene Kategorien verarbeitet werden 1 . Die anvisierte Wirkung – Wählersegmente mit maßgeschneiderten Halbwahrheiten zu bombardieren – könne also fortbestehen, indem man etwa Persönlichkeitsprofile über Likes und Klicks ableitet (statt offiziell „politische Meinung“ zu verwenden) 20 . Diese Kontroverse zeigt: **Die Regulierung befindet sich in einem Wettlauf mit der Technik.** Während Gesetze versuchen, *Missbrauchsschablonen* der Vergangenheit abzustellen, entwickeln Akteure neue Methoden, um Regeln zu umgehen. Nichtsdestotrotz bilden DSA und die neue EU-Werbeverordnung einen realen Rahmen, der das Szenario von *Projekt Klarblick* glaubwürdig untermauern kann – sei es als Hintergrund, in dem Konzerne und Kampagnen strategisch agieren, oder sogar als Plot-Element (Stichwort: ein Tech-Unternehmen unter regulatorischem Druck, ein Daten-Leck in der Ad-Bibliothek etc.).

KI-gestützte Kommunikation und politische Meinungsbildung

Chatbots im Wahlkampf: Künstliche Intelligenz verändert die politische Kommunikation grundlegend. Immer mehr **Chatbots** und automatisierte Dialogsysteme kommen zum Einsatz – sowohl auf Seiten der Wählerinformation als auch in der direkten Wähleransprache. Ein positives Beispiel ist *Wahl.Chat*, ein KI-gestützter Chatbot, den deutsche Doktoranden in Cambridge entwickelt haben, um unentschlossenen Wählern programmatisch Auskunft über Parteipositionen zu geben 21 . Anstatt hunderte Seiten Wahlprogramm zu wälzen, kann ein Bürger den Chatbot fragen: „*Was will Partei X in der Bildungspolitik?*“ – und erhält eine Antwort in verständlicher Sprache, basierend auf den Originalquellen 22 23 . Solche Tools sollen Politik **zugänglicher** machen und könnten die klassische Wahlentscheidungshilfe (z.B. den Wahl-O-Mat) ergänzen. Denkbar ist in naher Zukunft auch, dass Parteien offizielle Chatbots bereitstellen, die rund um die Uhr Fragen beantworten oder individualisierte Argumente liefern, um unentschlossene Wähler noch zu überzeugen. In ersten Ansätzen passiert das bereits über Messenger-Dienste und soziale Medien, wo automatisierte Accounts auf Bürgeranfragen reagieren. Allerdings stellt sich hier die Frage der **Objektivität**: Entwickler wie Michel Schimpf von *Wahl.Chat* betonen die Schwierigkeit, einen politischen Chatbot *hundertprozentig neutral* zu halten 24 – ein Thema, das in Medien und Fachkreisen intensiv diskutiert wird.

Propaganda-Bots und Social Bots: Während Chatbots offiziell zur Information dienen können, werden *inoffizielle* Bots missbraucht, um Meinungen zu beeinflussen. In sozialen Netzwerken existieren zahllose **Fake-Accounts**, die automatisiert Inhalte posten und menschliche Nutzer imitieren. Neuere KI-Modelle (etwa GPT-3/4) ermöglichen es, diese Bot-Postings noch überzeugender zu gestalten – mit kaum sprachlichen Fehlern und angepasstem Tonfall, so dass die Grenzen zwischen echter Graswurzel-Stimmung und künstlich erzeugtem *Astroturfing* verschwimmen. Ein aktueller Fall machte Anfang 2025 in Deutschland Schlagzeilen: Elon Musk persönlich lud die AfD-Politikerin Alice Weidel zu einem Live-Talk auf X/Twitter ein und bekräftigte dabei seine Wahlunterstützung für sie ²⁵. Gleichzeitig wurde bekannt, dass auf X seit Monaten eine koordinierte Kampagne pro AfD lief, bei der zahllose Bot-Accounts im Minutentakt rechtsradikale Parolen absetzten ²⁶. Diese Beiträge – unterstützt durch einen algorithmischen Boosting-Mechanismus – erzielten enorme Sichtbarkeit, ohne dass klar war, wie viel davon authentischer Zuspruch war. Solche Vorfälle verdeutlichen, dass **KI-gestützte Meinungsmache** längst Realität ist: *Social Bots*, befeuert durch lernende Algorithmen, können Trends und Debatten beeinflussen, indem sie die Illusion einer Mehrheit oder einer gewissen Stimmung erzeugen. Populistische Akteure weltweit gelten inzwischen als Meister darin, mit KI-generierten bzw. manipulierten Bildern und Videos kontroverse Emotionen zu schüren ²⁷. Durch die Flut an emotionalisierten, polarisierenden Narrativen werden die **Informationsräume der sozialen Medien gezielt geflutet** ²⁷. KI wirkt hier wie ein Brandbeschleuniger, der Tempo und Intensität von Desinformationskampagnen steigert. Diese Entwicklung ruft Sicherheitsbehörden auf den Plan: Das deutsche BSI warnt vor den Bundestagswahlen ausdrücklich, dass gegnerische Staaten oder politisch motivierte Gruppen Deepfakes und Bot-Netzwerke einsetzen könnten, um die öffentliche Meinung zu manipulieren ²⁸.

Psychometrisches Profiling 2.0: Ein weiterer Aspekt der KI-gestützten Meinungsbeeinflussung ist die Verfeinerung des **psychometrischen Profilings**. Darunter versteht man die Analyse von Persönlichkeitsmerkmalen, Einstellungen und Verwundbarkeiten einer Person anhand ihres digitalen Fußabdrucks, um maßgeschneiderte Botschaften zu entwerfen. Cambridge Analytica nutzte einst Facebook-Likes, um Rückschlüsse auf Big-Five-Persönlichkeitsprofile zu ziehen und entsprechend zugeschnittene Wahlwerbung auszuspielen. Heute erlauben moderne KI-Systeme eine noch umfangreichere Auswertung: Aus einer Kombination von Social-Media-Posts, Suchanfragen, Einkaufsdaten und sogar biometrischen Spuren (z.B. Stimmton in Sprachnachrichten) könnten Algorithmen *individuelle Propaganda* formulieren, die exakt auf die Psyche einer Zielperson abzielt. Forschungsberichte warnen, dass solche psychometrisch informierten KI-Bots sehr überzeugend sein könnten – sie kennen die *unbewussten Trigger* ihrer Adressaten und könnten diese gezielt ansprechen ²⁹ ³⁰. Bislang gibt es wenige bestätigte Fälle vollständig automatisierter 1:1-Beeinflussung, doch die Kombination aus **unreguliertem Datenhunger** und **generativer KI** lässt dieses Szenario plausibel erscheinen. Im US-Wahlkampf 2024 wurde z.B. bekannt, dass manche Kampagnen KI-Tools nutzten, um anhand von Wählerdaten die effektivsten Argumente für verschiedene Zielgruppen vorherzusagen (etwa welche Slogans bei klimabesorgten Vorstadtbewohnern vs. wirtschaftsorientierten Landbewohnern jeweils ziehen). Hier verschwimmen Microtargeting und KI-Kommunikation endgültig: Die *Maschine* hilft, für jede Teil-Öffentlichkeit ein anderes Gesicht der Realität zu erzeugen.

Meinungsbildung am Scheideweg: All diese Entwicklungen werfen die Frage auf, ob demokratische **Willensbildung** in der digitalen Ära noch ungestört funktionieren kann. Optimisten hoffen, dass aufgeklärte Bürger KI-gestützte Manipulation durchschauen werden und dass *Counter Speech* sowie Faktenchecks die Wirkung abmildern. Pessimisten – darunter renommierte Medienethiker – sehen hingegen die Gefahr einer *postfaktischen Kakophonie*, in der objektive Fakten untergehen. In der Tat haben Studien gezeigt, dass visuell überzeugende Deepfakes das Vertrauen der Bürger erschüttern könnten, *selbst wenn* sie als Fakes erkannt werden – weil irgendwann **generelles Misstrauen** entsteht, ob Bilder und Zitate überhaupt echt sind ³¹ ³². Noch blieb im Wahljahr 2024 der befürchtete *Deepfake-Sturm* aus – viele KI-Bilder waren schlecht genug erkennbar, sodass ein Teil der Bevölkerung

sie nicht ernst nahm ³³. Aber die Technologie entwickelt sich rasant weiter. Gesellschaft und Gesetzgebung stehen vor der Herausforderung, eine Balance zu finden: **Wie kann man die Vorteile KI-basierter politischer Kommunikation nutzen, ohne die Meinungsfreiheit und Wahrheitsfindung zu gefährden?** Diese offenen Fragen bilden einen spannenden Hintergrund für „Projekt Klarblick“, das solche Konflikte im fiktionalen Raum ausloten kann. Experten in der realen Welt fordern jedenfalls bereits, generative KI als „Hochrisiko-Technologie“ für demokratische Prozesse einzustufen, die besonderer Aufsicht und ggf. Einschränkungen bedarf ²⁷.

Zivilgesellschaftliche und journalistische Reaktionen

Medienethik und Aufklärung: Die rasanten technischen Entwicklungen haben eine breite Gegenbewegung in Zivilgesellschaft, Medien und Bildungssystem angestoßen. 2024 wurde in Deutschland zum Beispiel das Projekt „Jahr der Nachricht“ gestartet – eine Initiative, die sich ganz der Stärkung von Nachrichtenkompetenz und seriösem Journalismus widmet ³⁴. Unter Federführung von #UseTheNews und unterstützt durch Bundesbehörden soll dabei insbesondere jungen Menschen vermittelt werden, *Desinformation zu erkennen, Quellen zu prüfen* und Qualitätsmedien von Clickbait zu unterscheiden ³⁴. Solche Bildungsinitiativen greifen das Thema **Medienkompetenz** offensiv auf, oft in kreativen Formaten. Ein Highlight ist das Streaming-Format „Fake Train“ der Bundeszentrale für politische Bildung: In dieser Webserie begibt sich YouTube-Star **Rezo** mit prominenten Gästen auf eine Zugreise und bespricht unterwegs anschaulich Fälle von Fake News und Manipulation im Netz ³⁵ ³⁶. Spielerisch sollen so Jugendliche und junge Erwachsene für die Mechanismen von Desinformation sensibilisiert werden. Die Resonanz ist positiv – Formate wie *Fake Train* zeigen, dass Aufklärung auch auf Instagram, YouTube & Co stattfinden kann, genau dort also, wo die Problemzonen liegen. Auch in anderen Ländern gibt es vergleichbare Ansätze, z.B. kombinierte Schulungen von NGOs und Journalisten, um „News Literacy“ in Lehrpläne zu bringen. Kurz: Die **Zivilgesellschaft** hat erkannt, dass Prävention der beste Schutz vor Meinungsmache ist – ein informierter Bürger fällt seltener auf plump personalisierte Propaganda herein.

Faktenprüfung und investigativer Journalismus: Parallel dazu haben **Medienhäuser** ihre Anstrengungen verstärkt, Desinformation aktiv entgegenzutreten. Viele große Redaktionen betreiben inzwischen eigene **Faktencheck-Teams**, die virale Behauptungen prüfen und Ergebnisse öffentlich machen, oft in Zusammenarbeit mit internationalen Netzwerken. Beispielsweise kooperierten zur Europawahl 2024 verschiedene deutsche Medien und Recherchebüros, um kursierende Falschmeldungen zentral zu entkräften. Öffentlich-rechtliche Sender wie ARD und ZDF haben Formate wie den *Faktenfinder* oder *Scam-Report* etabliert, die im Fernsehen und online über aktuelle Fake-Themen aufklären. Wichtig ist dabei, das Vertrauen des Publikums zu behalten: Medien diskutieren intensiv, wie sie transparent mit eigenen Fehlern umgehen und wie KI in Redaktionen zum Einsatz kommen darf. Es gibt erste **Richtlinien** (etwa bei Nachrichtenagenturen), die den Einsatz von KI-Tools für Texte oder Bilder nur unter strengen Qualitätskontrollen zulassen. Zudem haben einige Verlagshäuser angekündigt, KI-generierte Inhalte stets zu kennzeichnen, um Glaubwürdigkeit nicht zu verspielen – ähnlich dem Prinzip, das man von Symbolen für Bildmanipulation kennt. Insgesamt wird der Journalismus seiner Rolle gerecht, *Korrektiv der Demokratie* zu sein: Durch **sachliche Berichterstattung** und das Einordnen von Falschmeldungen – etwa via dedizierter Faktenprüfer-Kolumnen – wirken seriöse Medien der Verbreitung irreführender Informationen entgegen ³⁷. Natürlich stehen sie dabei in Konkurrenz mit der Flut an Social-Media-Inhalten; umso wichtiger sind kollaborative Ansätze, die Reichweite schaffen (z.B. gemeinsame Aktionen mit Influencern oder Social-Media-Kampagnen unter dem Hashtag #StopFakeNews).

Technische Gegenmaßnahmen: Auch technisch wird zurückgeschlagen. Verschiedene Forschungsprojekte widmen sich der *Deepfake*-Erkennung – teils mit KI selbst. So werden Tools entwickelt, die manipulierte Videos oder synthetische Gesichter zuverlässig markieren können. Diese

Technik steht allerdings ebenfalls in einem Wettrennen mit immer besseren Fälschungen. Ein weiterer Ansatz ist die **Nachverfolgbarkeit** von Inhalten: Initiativen arbeiten an digitalem Wasserzeichen und *Content Credentials*, die anzeigen, ob ein Medieninhalt vom Originalautor stammt oder verändert wurde. Branchenübergreifend (Medienunternehmen, IT-Firmen, Behörden) gibt es Bündnisse, um solche Standards einzuführen. In der EU ist dazu auch im Gespräch, KI-Erzeugnisse ab einer gewissen Reichweite kenntlich zu machen – ein Thema im kommenden AI Act. Zivilgesellschaftliche Organisationen wie *AlgorithmWatch* oder *Mozilla Foundation* haben in der Vergangenheit Browser-Erweiterungen bereitgestellt, mit denen Nutzer z.B. politische Anzeigen, die ihnen gezeigt werden, sammeln und anonymisiert zur Forschung bereitstellen konnten. Zwar stießen solche Projekte manchmal auf rechtliche Hürden (etwa das Facebook-Nutzungsverbot solcher Tools), doch der DSA könnte hier neue Chancen eröffnen, indem er **Datenzugang für öffentliche Forschung** garantiert. Insgesamt gilt: Auf Seiten der „Guten“ werden immer neue Ideen geboren, um den „Bösen“ nicht kampfflos das Feld zu überlassen – sei es durch Aufklärung, Faktenchecks oder technische Hilfsmittel.

Neue Plattform-Modelle: Interessant ist in diesem Zusammenhang der Ruf nach *alternativen Räumen* für Online-Debatten. Einige Medienethiker und Netzaktivisten fordern eine **Entkommerzialisierung** zentraler digitaler Infrastrukturen, um dem Profitmotiv – das oft extreme, polarisierende Inhalte begünstigt – den Boden zu entziehen ³⁸ ³⁹. Eine konkrete Umsetzung ist das internationale Projekt **„Public Spaces Incubator“ (PSI)**, an dem sich öffentlich-rechtliche Medienhäuser aus Europa und darüber hinaus beteiligen ⁴⁰. Unter Federführung von u.a. ZDF, ARD (seit Oktober 2024), der belgischen RTBF und Radio-Canada wird daran gearbeitet, **nicht-kommerzielle soziale Plattformen** zu schaffen ⁴⁰ ⁴¹. Diese sollen konstruktive Diskussionsräume jenseits der großen Silicon-Valley-Netzwerke bieten, wo Algorithmen nicht auf maximale Verweildauer oder Empörung optimiert sind, sondern auf inhaltliche Vielfalt und respektvollen Austausch. Solche Experimente stehen noch am Anfang, könnten aber langfristig zu einer *öffentlich-rechtlichen Alternative* zu Facebook, YouTube und Co. führen. Für *Projekt Klarblick* eröffnet dies interessante Szenarien: Etwa eine Handlung, in der sich Akteure auf einer unabhängigen Plattform formieren, während auf den großen Plattformen das Chaos tobt – oder Konflikte zwischen einem staatlichen „Klarblick-Netz“ und den etablierten Diensten. Realitätsnah ist die Idee jedenfalls, denn die beschriebenen Ansätze existieren bereits im Keim.

Behördliche Wachsamkeit: Schließlich sei erwähnt, dass auch staatliche Stellen sich besser wappnen. Sicherheitsbehörden (Verfassungsschutz, BKA etc.) kooperieren verstärkt, um **Wahlmanipulationskampagnen** früh zu erkennen. Sie informieren die Öffentlichkeit proaktiv – wie das BSI, das in Newsletter betont, dass das amtliche Endergebnis einer Wahl nicht hackbar ist (Stichwort: Papierstimmzettel) ⁴², um Verschwörungstheorien den Nährboden zu entziehen. Zudem werden verdächtige Aktivitäten im Netz beobachtet und – soweit gesetzlich möglich – unterbunden. Das Netzwerkdurchsetzungsgesetz (NetzDG) in Deutschland wurde 2024 an den DSA angepasst, bleibt aber ein Werkzeug gegen strafbare Inhalte im Netz. Europol hat ein eigenes Center zur Bekämpfung von Desinformation im Rahmen von hybriden Bedrohungen. Und nicht zuletzt finden auf diplomatischer Ebene Gespräche mit den großen Plattformbetreibern statt: Man versucht, **Vertrauensbeziehungen** aufzubauen, damit bei akuten Desinformationswellen schnell reagiert werden kann. Dies alles zeigt: Das Thema ist in der **gesamtgesellschaftlichen** Agenda angekommen. Es gibt einen Wettstreit zwischen *Disruptoren* und *Bewahrern* der Demokratie, der hervorragenden narrativen Stoff bieten kann.

Fazit: Realitätsnahe Bausteine für "Projekt Klarblick"

Abschließend lässt sich festhalten, dass zahlreiche der oben skizzierten Entwicklungen sich hervorragend als **reale Grundlage** für das fiktionale Szenario in „Projekt Klarblick“ eignen. Im Einzelnen könnten folgende Elemente aus der echten Welt in der Geschichte verarbeitet werden:

- **Microtargeting und personalisierte Desinformation:** Etwa eine geheime Wahlkampagne, die mithilfe gestohlener Nutzerdaten jeder Wählergruppe andere *Wahrheiten* vorspiegelt – inspiriert von realen Fällen à la Cambridge Analytica oder der Saral-App in Indien. Die Story könnte zeigen, wie solche *maßgeschneiderten Lügen* einzelne Charaktere in die Irre führen, was perfekt die Gefahren dieses Trends illustriert.
- **KI-generierte Deepfakes und Bots:** Ein Szenario-Highlight könnte ein Deepfake-Skandal sein – beispielsweise taucht ein kompromittierendes Video eines Kandidaten auf, das sich als KI-Fälschung entpuppt (nach Vorbild des Merz-Videos ³). Auch **Bot-Armeen** in sozialen Netzwerken, die die öffentliche Meinung zu kippen drohen, bieten Spannungspotenzial. Diese Elemente machen die Bedrohung durch KI greifbar und basieren auf realen Phänomenen.
- **Plattformregulierung und Gesetzeskonflikte:** Der **Digital Services Act** und die neuen EU-Regeln zu politischer Werbung könnten im Hintergrund des Plots wirksam sein. Beispielsweise könnte eine Tech-Firma in *Projekt Klarblick* versuchen, ihre Algorithmen zu verstecken oder eine Wahlkampftruppe sucht gezielt nach *Schlupflöchern* in den Vorschriften. Das schafft Realismus und ermöglicht dramatische Konflikte zwischen Reformern und Profiteuren des alten Wildwest-Internet.
- **KI-Chatbots & psychometrisches Profiling:** Ein fiktiver Wahlkampf in *Klarblick* könnte realitätsnah einen **KI-Berater** zeigen, der dem Kandidaten exakt vorgibt, was er welchem Publikum sagen soll – gestützt auf psychologische Profile der Wähler. Ebenso denkbar: Ein Chatbot tritt als vermeintlicher *freundlicher Helfer* auf, manipuliert aber im Hintergrund die Nutzer subtil. Diese Motive greifen aktuelle Technik auf und führen sie konsequent weiter.
- **Zivilgesellschaftliche Gegenwehr:** Schließlich kann die Geschichte auch die positiven Gegenkräfte widerspiegeln. Etwa eine Gruppe von Journalisten, die im Stil realer *Faktenchecker-Teams* einer Verschwörung auf die Spur kommt, oder eine junge Protagonistin, die durch ein Medienkompetenz-Projekt (*analog zu "Fake Train" mit Rezo*) gelernt hat, Fakes zu entlarven, und nun ihr Wissen einsetzt. Solche Helden orientieren sich an der Wirklichkeit und geben dem Leser Hoffnung, dass Aufklärung möglich ist.

All diese Punkte zeigen: Die **wichtigsten Entwicklungen der Gegenwart** – von KI-Microtargeting über Plattformregulierung bis hin zu ethischen Debatten – liefern reichhaltiges Material, um „Projekt Klarblick“ in einem glaubwürdigen, aktuellen Kontext anzusiedeln. Indem der fiktionale Plot diese realen Elemente aufgreift, bleibt er für das Publikum **nachvollziehbar** und **relevant**. Die Herausforderungen unserer digitalen Demokratie im Mai 2025 können so im Spiegel der Fiktion noch eindringlicher erlebt und reflektiert werden. ⁴ ¹

- 1 19 20 **Political advertising: EU won't ban voter manipulation and microtargeting – Patrick Breyer**
<https://www.patrick-breyer.de/en/political-advertising-eu-wont-ban-voter-manipulation-and-microtargeting/>
- 2 **'Wild West': Republican video shows AI future in US elections | Joe Biden News | Al Jazeera**
<https://www.aljazeera.com/news/2023/4/28/wild-west-republican-video-shows-ai-future-in-us-elections>
- 3 4 5 31 32 **Künstliche Intelligenz: KI im Superwahljahr**
<https://www.freiheit.org/de/deutschland/ki-im-superwahljahr-revolution-oder-bekannte-bedrohung-im-neuen-gewand>
- 6 **Google to require disclosure of AI use in political ads - POLITICO**
<https://www.politico.com/news/2023/09/06/google-ai-political-ads-00114266>
- 7 8 10 **The Digital Services Act Is Fully In Effect, But Many Questions Remain | TechPolicy.Press**
<https://techpolicy.press/the-digital-services-act-in-full-effect-questions-remain>
- 9 **The EU's Digital Services Act**
https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en
- 11 14 15 **Digital Services Act (DSA) | Updates, Compliance, Training**
<https://www.eu-digital-services-act.com/>
- 12 13 16 17 18 **EU introduces new rules on transparency and targeting of political advertising - Consilium**
<https://www.consilium.europa.eu/en/press/press-releases/2024/03/11/eu-introduces-new-rules-on-transparency-and-targeting-of-political-advertising/>
- 21 22 23 24 **Politik per Klick: Dieser KI-Chatbot hilft auch unentschlossenen Wählern | Euronews**
<https://de.euronews.com/my-europe/2025/02/19/politik-per-klick-dieser-ki-chatbot-hilft-auch-unentschlossenen-waehlern>
- 25 26 27 **„Künstliche Intelligenz im Wahlkampf ist Hochrisikotechnologie...**
<https://publikationen.bibliothek.kit.edu/1000179275>
- 28 42 **BSI - Bundesamt für Sicherheit in der Informationstechnik - Newsletter SICHER • INFORMIERT vom 30.01.2025**
https://www.bsi.bund.de/SharedDocs/Newsletter/DE/BuergerCERT-Newsletter/02_Sicher-Informiert_30-01-2025.html
- 29 30 **Psychometric Profiling of Digital Voter Data • Software Freedom Law Center, India**
<https://sflc.in/psychometric-profiling-of-digital-voter-data/>
- 33 **AI is helping shape the 2024 presidential election in an unexpected way | AP News**
<https://apnews.com/article/artificial-intelligence-memes-trump-harris-deepfakes-256282c31fa9316c4059f09036c70fa9>
- 34 **Mit dem "Jahr der Nachricht" gegen Desinformation | Bundesregierung**
<https://www.bundesregierung.de/breg-de/aktuelles/gegen-desinformationen-jahr-der-nachricht-2264110>
- 35 36 **Streaming-Format "Fake Train" zu Desinformation | Bundesregierung**
<https://www.bundesregierung.de/breg-de/aktuelles/bpb-fake-train-2290552>
- 37 **Fakten gegen Desinformationen - Die Bundeswahlleiterin**
<https://www.bundeswahlleiterin.de/europawahlen/2024/fakten-desinformation.html>
- 38 39 40 41 **Sprache als Pfeiler der Demokratie - M - Menschen Machen Medien (ver.di)**
<https://mmm.verdi.de/aktuelle-meldungen/sprache-als-pfeiler-der-demokratie-101819/>