Big Brother und die Sozialen Medien

Ein früherer Mitarbeiter von Facebook hat sich mal verbittert darüber geäußert, dass die hellsten Köpfe seiner Generation darüber nachdenken, wie man Menschen dazu bringt, auf Werbebanner zu klicken.[1] Weil sie extrem viele Daten haben und sehr gut bezahlen, ziehen die großen Internetfirmen tatsächlich viele Talente aus den Bereichen Statistik, maschinelles Lernen und KI an. Und ihre Arbeit macht einen Unterschied: Die Werbung, die wir online sehen, ist durch KI daraufhin optimiert, dass sie uns beeinflusst.

Diese Beeinflussung kann harmlos sein, zum Beispiel wenn ich Werbung für ein Buch angezeigt bekomme, das mich interessiert und das ich vielleicht sonst nie entdeckt hätte. Die Werbung hat dann eine rein informierende Wirkung und ich entscheide mich bewusst zum Kauf. Es ist die Möglichkeit einer unbewussten Beeinflussung, die uns Angst macht. Bei Fernsehwerbung oder Zeitungsanzeigen sind wir da weniger ängstlich. Trotzdem glauben viele Menschen daran, dass wir durch Werbung unbewusst manipuliert werden können. Würde Werbung nicht wirken, würde wohl kaum so viel Geld dafür ausgegeben. Aber in welchem Maß können wir beeinflusst werden, ohne dass wir das merken?

Werden wir unbewusst manipuliert?

Obwohl sie vielfach widerlegt worden ist, hält sich die moderne Legende von einem Experiment in den 1950er Jahren, bei dem während eines Kinofilms ganz kurz und unbemerkt die Aufforderung ›Trink

1 Das Zitat von Jeff Hammerbacher lautet: »The best minds of my generation are thinking about how to make people click ads. That sucks.« (Vance, 2017)

Coca-Cola‹ eingeblendet wurde, und die Kinobesucher in der Pause deshalb deutlich mehr Cola gekauft haben sollen. Es ist aufgrund von Laborstudien in der Psychologie nicht vollständig auszuschließen, dass so etwas funktionieren könnte, aber niemand hat es bisher geschafft, Bedingungen außerhalb des Labors herzustellen, bei denen jemand von einem Reiz beeinflusst wird, von dem er gar nichts weiß. Falls es überhaupt einen Einfluss eines solchen unbewussten Reizes auf das Verhalten gibt, ist er extrem klein. Das Ziel von Werbung ist normalerweise nicht, nicht wahrgenommen zu werden, sondern im Gegenteil, möglichst viel Aufmerksamkeit zu erregen.[2]

Wenn wir also nicht direkt durch unbewusste Botschaften beeinflusst werden können, wie beeinflusst uns Werbung dann? Kauft man im Supermarkt Zahnpasta, insbesondere wenn man es eilig hat, denkt man nicht lange darüber nach, welche Marke man nimmt. Die meisten Menschen kaufen einfach aus Gewohnheit immer dieselbe Marke. Der Preis ist natürlich auch wichtig. Aber wenn man die Wahl zwischen zwei Zahnpasten hat und nur die eine kennt und mit positiven Eigenschaften verbindet, weil sie gut und oft beworben wurde, für welche entscheidet man sich wohl? In diesem Moment ist einem nicht unbedingt bewusst, dass die Kaufentscheidung auch durch die Werbung beeinflusst wurde. Trotzdem weiß jeder, dass Werbung so funktioniert.

Im Jahr 2014 ist ein Shitstorm über Facebook hereingebrochen, als in einem wissenschaftlichen Artikel von einem Experiment berichtet wurde, in dem Facebook ohne Wissen der Nutzer versucht hat, ihre Stimmung zu beeinflussen.[3] Hat ein Facebooknutzer viele Freunde und ist in vielen Gruppen Mitglied, produzieren seine Freunde und Gruppen mehr Posts als er lesen kann. Die Neuigkeiten, die er auf seiner Facebookseite sieht, werden daher (Überraschung!) von einem Algorithmus ausgewählt. Für über 600.000 zufällig ausgewählte Nutzer wurde dieser Algorithmus während dieses Experimentes leicht geändert. Zuerst wurden die Posts ihrer Freunde auf emotionale Wörter analysiert: Kommt zum Beispiel das Wort ›glücklich‹ oder das Wort ›traurig‹ darin vor? Danach wurde eine Woche lang für eine Gruppe ein Großteil der positiven Posts unterdrückt und für eine andere Gruppe ein Großteil der negativen Posts. In weiteren Kontrollgruppen wurden

2 Siehe Moore (1982).

3 Die Studie wurde von Kramer, Guillory & Hancock (2014) durchgeführt. Die heftigen Reaktionen darauf wurden z.B. von Booth (2014) beschrieben.

zufällig Neuigkeiten unterdrückt. Würden Nutzer, die weniger Posts ihrer Freunde sehen, die positive Gefühle ausdrücken, auch selber weniger positive Posts posten? Die Antwort ist: ja. Der Effekt ist aber äußerst klein. Von 1.000 Wörtern, die jemand auf Facebook postet, sind im Durchschnitt 52 positiv. Durch die Manipulation sind es nur noch 51.

Es wäre überraschend gewesen, wenn der Effekt größer gewesen wäre, denn die Stimmung eines Nutzers hängt nicht nur davon ab, was er bei Facebook liest. Auf ganz Facebook hochgerechnet geht es trotzdem noch um hunderttausende Posts pro Tag, die weniger positiv besetzte Wörter nutzen. Amüsiert ein Freund sich über ein Video, dann kann ich nicht antworten, dass ich das auch lustig finde, wenn ich seinen Post gar nicht zu sehen bekomme. Es ist deshalb auch kein Wunder, dass es durch diese Manipulation weniger positive Posts gibt.

Mich haben die heftigen Reaktionen auf diese Studie erstaunt. Natürlich kontrolliert Facebook, was Sie auf Facebook sehen. Natürlich macht Facebook die ganze Zeit Experimente mit seinen Nutzern, um seine Empfehlungs- und Werbealgorithmen zu verbessern (A/B-Tests wie bei Netflix). Natürlich hat Facebook ein Interesse daran, dass Sie Facebook möglichst viel Aufmerksamkeit widmen, damit Sie auch möglichst viel relevante Werbung sehen. Und natürlich interessiert sich Facebook deshalb auch für die Gefühle seiner Nutzer. Warum also der Aufruhr?

Selbst wenn man verstanden hatte, dass Facebook mit Werbung Geld verdient, war Vielen offenbar noch nicht klar, dass Facebooks Algorithmen nicht nur kontrollieren, welche Werbung wir sehen, sondern auch welche sonstigen Inhalte. Das betrifft neben belanglosen Urlaubsfotos von Freunden auch Nachrichten und Fake News. Dass Facebook unsere Stimmungen ohne unser Wissen manipulieren könnte, ist ein beängstigender Gedanke. Und dass eine künstliche Intelligenz, die wir weder kennen noch verstehen, schon längst herausgefunden haben könnte, wie man uns am besten unbewusst manipuliert, verstärkt die Angst noch mehr. Anders als bei Werbung, bei der man immer weiß, dass der Versuch einer Beeinflussung unternommen wird, und die entsprechend gekennzeichnet werden muss, wurden die Nutzer in der Facebookstudie nicht genügend darüber aufgeklärt. Die Nutzer auf Facebook haben solchen Experimenten zwar formell mit den Nutzungsbestimmungen zugestimmt, aber bewusst war es ihnen nicht, dass Facebook versuchen könnte, ihre Stimmung zu beeinflussen.

Wahlwerbung und Propaganda nutzen Daten

Doch der richtig große Shitstorm sollte erst noch kommen. Was, wenn Facebook nicht nur die emotionale Stimmung seiner Nutzer mit Katzenvideos manipuliert, sondern auch die politische Stimmung beeinflusst? Hat Facebook neben dem Verkauf von Werbung noch andere, vielleicht politische Interessen, von denen wir nichts wissen? Welche Absichten haben Facebooks Kunden? Können auch Geheimdienste oder zwielichtige Akteure sich Facebooks Daten zunutze machen? Kennt man die politischen Überzeugungen von ausreichend vielen Menschen und besitzt außerdem ihre Facebookdaten, lässt sich durch Statistik und maschinelles Lernen berechnen, wie wahrscheinlich es ist, dass zum Beispiel jemand, der über 50 ist, im Ruhrgebiet wohnt und die Facebookseiten von DGB und Herbert Grönemeyer mag, die SPD wählt. Das ist eine leichte Übung. Statt nur Wahlplakate in Bochum zu kleben, kann man diese Person gezielt online mit maßgeschneiderten Botschaften ansprechen. Das nennt man ›Microtargeting‹. Und genau solche Daten für Microtargeting hat die Beratungsfirma Cambridge Analytica gesammelt. Teils auf legalem, teils auf illegalem Weg. Der Verdacht steht im Raum, dass die Wahlerfolge der Leave-Kampagne beim Brexit-Referendum und von Donald Trump bei der Präsidentschaftswahl 2016 durch solche Datenanalysen beeinflusst wurden.[4]

Wir wissen nicht, wie viel effektiver als normale Wahlwerbung dieses Microtargeting war. Und da politische Stimmungen, genauso wie emotionale Stimmungen, von vielen Faktoren abhängen, ist es unwahrscheinlich, dass viele Menschen nur aufgrund der Facebook-Werbung von Cambridge Analytica Donald Trump statt Hilary Clinton gewählt haben. Aber wir wissen auch, dass Wahlen knapp ausgehen können. Es ist daher wichtig für eine Wahlkampagne, dass die eigenen Unterstützer wirklich wählen gehen und möglichst viele unentschiedene Wäh-

4 Man weiß gar nicht, wo man anfangen soll, wenn man über den Cambridge-Analytica-Skandal schreiben möchte. Der TED-Talk von Carole Cadwalladr, die den Skandal aufgedeckt hat, ist vielleicht ein guter Startpunkt (Cadwalladr, 2019). *The Guardian* hat eine Webseite mit allen Artikeln zu dem Thema eingerichtet (The Guardian, 2018). Eine ausführliche Erklärung von Microtargeting bietet auch die Bundeszentrale für politische Bildung an (Christl, 2019). Die Berliner Datenschutzbeauftragte mahnt derweil an, dass sich die deutschen Parteien bei ihrer Wahlwerbung an die Datenschutzgrundverordnung halten sollen, die das Erfassen von politischen Meinungen untersagt (Dachwitz, 2024).

ler das Kreuz an der richtigen Stelle machen. Um das sicherzustellen, gehört der Einsatz von Daten und Statistik schon sehr lange zu jedem Wahlkampf (und zur Wahlforschung) dazu.[5] In einem demokratischen Wettbewerb um Stimmen sind Informationen über die Meinungen der Wähler (und Nicht-Wähler) entscheidend. Ihre Bundestagsabgeordnete muss diese Meinungen kennen, wenn sie ihre Wähler verantwortungsvoll repräsentieren will. Man sollte nicht vergessen: Es ist die Aufgabe von Politikerinnen und Politikern zu informieren und zu überzeugen, und so Wahlentscheidungen zu beeinflussen. Big Data und KI könnten diese legitimen demokratischen Prozesse unterstützen.

Stattdessen scheinen im Netz heimlich Kampagnen in unbekanntem Ausmaß zu laufen. Wahlgesetze, die Obergrenzen für Wahlkampfausgaben setzen, werden auf diese Weise unterwandert, wie das wohl im Fall des Brexit-Referendums passiert ist. Zwielichtige Firmen bieten ihre Dienste zur Desinformation und Wahlmanipulation an. Mit und ohne deren Unterstützung untergraben außerdem fremde Regierungen die Meinungsbildung, wie das von Russland bei der Trump-Wahl 2016 vermutet wird. In Rumänien urteilte das Verfassungsgericht im Dezember 2024 sogar, dass die Präsidentschaftswahl wegen eines »russischen hybriden Angriffs« wiederholt werden muss.[6]

Systematische Desinformation und Fake News im großen Maßstab sind schlimm genug. Aber durch Big Data und KI lassen sich einzelne Menschen gezielt mit für sie maßgeschneiderten Informationen ansprechen. Es kann passieren, dass wir diese gezielte Manipulation nicht einmal bemerken. Und dass auch niemand anderes das mitbekommt und öffentlich widersprechen könnte. Propaganda und Desinformation erreichen durch Big Data und KI neue Dimensionen. Momentan sieht es allerdings nicht so aus, als ob die großen Tech-Unternehmen freiwillig die nötige Transparenz herstellen wollten.

---

5 In seinem umfassenden Buch über Automatisierung bespricht Pollock (1964) im letzten Abschnitt des letzten Kapitels die gesellschaftlichen Perspektiven auf das Thema. Schon damals machte er sich Sorgen darüber, dass die Anwendung von computergestützter Statistik den demokratischen Diskurs nicht unbedingt zum Besseren ändern wird.

6 Für die Wahlkampfausgaben siehe Cadwalladr, Graham-Harrison & Townsend (2018), für die zwielichtigen Firmen Coerper & Klauser (2023), für den russischen Einfluss Timberg (2017) und für die Wahl in Rumänien Zimmermann (2024).

Der Staat soll unsere Daten schützen

Wer dem Silicon Valley misstraut, dem bleibt nichts anderes übrig, als sich auf den Staat zu verlassen, dass er neue Regeln für die digitale Welt aufstellt. Die KI-Verordnung der Europäischen Union, die 2024 verabschiedet wurde, verbietet explizit den Einsatz von manipulativen Techniken, die bewusste Entscheidungen untergraben, sofern Menschen dadurch ein ernster Schaden entstehen könnte. Im Annex III der KI-Verordnung sind konkrete Beispiele für Anwendungen von KI-Systemen genannt, die zwar nicht verboten sind, aber als besonders riskant eingestuft werden und die daher besonderen Sorgfalts- und Transparenzpflichten unterliegen. KI-Systeme, die Wahlen beeinflussen sollen, indem sie einzelnen Wählern nur für sie bestimmte Informationen zuspielen, sind dort explizit genannt.

Die KI-Verordnung ergänzt bestehende Gesetze um Aspekte, die spezifisch für KI sind. Weil aber niemand alle potenziell problematischen Anwendungen vorhersehen kann, definiert die Verordnung die Risiken unabhängig von konkreten Anwendungen. Wer KI-Produkte anbietet, muss nachweisen, dass er bei Entwicklung und Anwendung verantwortungsvoll vorgeht. Dafür gibt es eine Einteilung von geringem zu hohem Risiko. Diese Risikogruppen sind recht abstrakt beschrieben. Anwendungen ohne erkennbares Risiko sind nicht genau definiert, aber auch nicht betroffen. Für die anderen wird sich ein System von Normen und Zertifizierungen etablieren, das Firmen dabei hilft, Risiken zu managen. Und weil wir in Deutschland gut im Normieren sind, wird nicht erst seit der Verabschiedung der KI-Verordnung an DIN-Normen für KI gearbeitet.[7] Es ist nur noch eine Frage der Zeit, bis es einen TÜV für KI-Anwendungen geben wird.

KI wird dabei nicht anderes behandelt als jede andere Technologie, die auch normiert, zertifiziert und abhängig vom Grad der Risiken erst zugelassen werden muss. Da sind KI-Produkte nicht anders als Fahrzeuge, Medizintechnik oder Finanzprodukte. Diese Produkte müssen ohnehin einen Zulassungsprozess durchlaufen – egal, ob in diesen Produkten KI steckt oder nicht. Da KI aber in vielen verschiedenen, vielleicht noch nicht existierenden Produkten eingesetzt werden kann, sah die EU eine Regelungslücke. Das selbst gesteckte Ziel der EU war dabei, Innovation nicht durch Überregulierung zu erschweren, aber ihre Bür-

7 Siehe DIN & DKE (2022).

ger trotzdem vor potenziell gefährlichen Anwendungen zu schützen. Der bereits erwähnte Annex III ist eine erweiterbare Liste, die konkrete Beispiele für Anwendungen gibt, die als besonders riskant einzuschätzen sind. Neben Systemen, die Wahlen beeinflussen sollen, finden sich da zum Beispiel Systeme zur Personalauswahl oder zur Feststellung der Kreditwürdigkeit:

In Deutschland darf niemand aufgrund von Geschlecht, Rasse oder ethnischer Herkunft, Religion oder Weltanschauung, Behinderung, Alter oder sexueller Identität benachteiligt werden. Dass Unternehmen KI-Systeme in Bewerbungsverfahren einsetzen, ändert nichts daran, dass sie sich an das Allgemeine Gleichbehandlungsgesetz halten müssen. Nehmen wir an, eine große Firma, die jedes Jahr tausende an Bewerbungen bekommt, hat über viele Jahre Statistik darüber geführt, welche Bewerber erfolgreich waren. Leider wurden in der Vergangenheit bei der Personalauswahl nicht immer alle gleich behandelt. Insbesondere Frauen wurden oftmals erst gar nicht zu Bewerbungsgesprächen eingeladen. Was passiert, wenn ein KI-System, das bei der Personalauswahl unterstützen soll, aus diesen Daten lernt, wer zu einem Vorstellungsgespräch eingeladen werden soll?[8] Gibt man oben diskriminierende Daten in das System hinein, kommen unten diskriminierende Entscheidungen raus. Das ist das DIDO-Prinzip: ›discrimination in, discrimination out.‹[9] Die KI-Verordnung wird hoffentlich dafür sorgen, dass Softwarehersteller, die anderen Unternehmen so eine Software zur Personalauswahl anbieten, die Verantwortung nicht an ihre Kunden abschieben. Und die Unternehmen, die so eine Software einsetzen, dürfen nicht davon ausgehen, dass die Gleichbehandlung schon gewährleistet sein wird.

Ähnliches gilt für den Einsatz von KI zur Feststellung der Kreditwürdigkeit. Die Schufa ist ein privates Unternehmen, das Daten über fast die gesamte Bevölkerung in Deutschland sammelt. Aus diesen Daten berechnet das Unternehmen den Schufa-Score, der vorhersa-

8 Das Beispiel ist nicht komplett hypothetisch. Amazon hat versucht so ein System zu entwickeln, dann aber gemerkt, dass das problematisch ist (Dastin, 2018).

9 Hamid Khan, der sich gegen rassistische Polizeiüberwachung in Los Angeles engagiert, spricht von »racism in, racism out« (Buranyi, 2017). Seine Variante des Informatiker-Mottos ›garbage in, garbage out‹ lässt sich natürlich auf andere Formen der Diskriminierung übertragen. Über Khan und die Koalition gegen Polizeiüberwachung, in der er sich engagiert, habe ich zuerst in dem Buch von Katz (2020) gelesen (S. 143ff.).

gen soll, ob eine Person ihren Zahlungsverpflichtungen nachkommen wird. Vermieter nutzen diesen Score bei der Auswahl von Mietern, Banken nutzen ihn zur Kreditvergabe und auch beim Abschluss eines Handyvertrages wird die Bonität geprüft. In Deutschland kann man der Datensammelwut der Schufa nur schwer entgehen, denn ohne eine Einwilligung zur Bonitätsprüfung bei der Schufa kann es bei der Wohnungssuche oder mit einer Zahlung auf Rechnung schwer werden. Genauso bei einem schlechten Schufa-Score. Wenn man keinen Kredit bekommt, würde man von der Schufa schon gerne erfahren, warum der Score so schlecht ist. Wie genau der Schufa-Score berechnet wird, ist aber Geschäftsgeheimnis.

Woher wissen wir, dass der Schufa-Score nicht diskriminierend ist? Welche Rolle spielt zum Beispiel das Alter bei der Einschätzung der Kreditwürdigkeit? Oder die Postleitzahl, weil die Kreditwürdigkeit im Durchschnitt in armen Wohngegenden geringer ist? Wie kann man bei dieser Intransparenz im Einzelfall überprüfen, ob vielleicht ein Datenfehler vorlag? Wenn der Kredit automatisch abgelehnt wird und man weiß nicht warum, gibt es dann überhaupt noch eine realistische Möglichkeit zum Einspruch? Nach der Europäischen Datenschutzgrundverordnung (DSGVO) sind automatisierte Entscheidungsverfahren in Fällen, die solch gravierende Folgen für einzelne Menschen haben können, nicht erlaubt. Der Europäische Gerichtshof hat 2023 festgestellt, dass der Schufa-Score nicht als maßgebliches Entscheidungskriterium dienen darf. Die Schufa wollte sich daher von ihren Kunden bescheinigen lassen, dass sie den Score nicht als alleiniges Kriterium einsetzen. Für den Online-Abschluss neuer Stromverträge wird ein Energieversorger aber wahrscheinlich gerade deshalb Bonitäts-Scores von der Schufa kaufen wollen, weil ihm keine anderen Informationen über Neukunden vorliegen. Wie kann er sonst online und vollautomatisch Verträge abschließen ohne zu wissen, ob der Kunde seine Rechnungen bezahlen wird?[10]

Natürlich wird die Schufa von der zuständigen Datenschutzbehörde kontrolliert. Diese könnte richtig saftige Strafen verhängen und in der KI-Verordnung sind die Strafen noch drakonischer. Aber nicht alle Behörden wollen oder können so richtig Biss entwickeln. Die irische Datenschutzbehörde, die für Facebook zuständig ist, verhängte zwar

10 Zum EuGH-Urteil siehe z.B. Robertz & Eßlinger (2023). Hintergründe zum Schufa-Score und dessen Einsatz finden sich bei Schreiber (2023).

mal eine Rekordstrafe von 1,2 Milliarden Euro gegen die Facebook-Firma Meta, aber erst, nachdem die Behörde von Gerichten dazu gezwungen wurde.[11]

Wer schützt uns vor dem Staat?

Eine große Ironie der Geschichte ist, dass wir nach dem Staat rufen, unsere Dateninteressen zu verteidigen. Doch es ist kein Zufall, dass das Wort ›Statistik‹ so ähnlich wie ›Staat‹ klingt. Staaten haben schon vor langer Zeit damit angefangen, Daten im großen Stil zu sammeln. Das Deutsche Statistische Bundesamt hört sich nach einer langweiligen Behörde an, ist aber eine unersetzliche Datenkrake. Bevölkerungsstatistiken sind zur Planung von Schulen, Renten oder Zuwanderung absolut notwendig und Wirtschafts- und Einkommensdaten werden zur Steuervorhersage benötigt. Genau wie Unternehmen auch mussten Staaten schon immer für die Zukunft planen und sie tun das (keine Überraschung!) mithilfe von Daten.

Das Volkszählungsurteil des Bundesverfassungsgerichts von 1983, das dem Staat bei der Datenerhebung über seine Bürger Einhalt gebietet, war ein Meilenstein für den Datenschutz in Deutschland. Ein Jahr vor *1984* schien Orwells Roman wohl ausgesprochen aktuell. Da wir heute aus Bequemlichkeit den großen Tech-Unternehmen erlauben, Unmengen an persönlichen Daten über uns zu sammeln, können wir die damalige Aufregung über die Volkszählung nicht mehr ganz nachvollziehen. In den 80er Jahren zog man in den Debatten um Datenschutz auch Lehren aus dem Dritten Reich, denn der Holocaust in seiner ungeheuerlichen Dimension wäre ohne eine straff organisierte staatliche Bürokratie nicht möglich gewesen. Dazu gehörte auch, dass der Staat genau Buch darüber führte, wer jüdischen Glaubens war und wo die Menschen wohnten. Auf den ersten Blick mögen diese Informationen als kein großes Geheimnis erscheinen, sie haben aber die Organisation von Massendeportationen immens erleichtert. Ein oft übersehenes Detail der Geschichte des Dritten Reichs ist, dass diese Daten nicht nur in Büchern, Akten und auf Karteikarten standen. Sie wurden auch auf Lochkarten gespeichert, damit sie maschinell verarbeitet wer-

11 Goujard & Scott (2023) geben einen Überblick. Der Fall ist bei Lomas (2023) genauer dokumentiert.

den konnten. So konnte die gewaltige Bürokratiemaschine im Nationalsozialismus effizient arbeiten. Die deutsche IBM-Tochterfirma DEHOMAG verkaufte ihre mechanischen Lochkartenmaschinen an das Statistische Reichsamt, die Wehrmacht und an das Rassenamt der SS, die auch die Daten von KZ-Häftlingen auf Lochkarten speicherte.[12]

Dass der Datenschutz in Deutschland eine höhere Bedeutung hat als in anderen Ländern, hängt sicher auch damit zusammen, dass die Erinnerung an das Ministerium für Staatssicherheit der DDR noch lebendig ist. Man mag sich gar nicht vorstellen, wie viel effizienter die Überwachung der Stasi mit den heutigen technischen Möglichkeiten gewesen wäre. Aus den Enthüllungen von Edward Snowden wissen wir, dass Nachrichtendienste diese Möglichkeiten ausgiebig nutzen und dabei eng mit den großen Tech-Unternehmen zusammenarbeiten. Die bereits erwähnte Rekordstrafe für Facebook von 1,2 Milliarden Euro wurde deshalb verhängt, weil Facebook die Daten seiner europäischen Nutzer nicht ausreichend vor dem Zugriff der amerikanischen Nachrichtendienste schützt.

Um ihre Bürger vor umfassender Überwachung zu schützen, setzt die KI-Verordnung der EU nicht nur der Wirtschaft Schranken beim Einsatz von KI-Methoden, sondern auch den Mitgliedsstaaten. Besonders umstritten ist der Einsatz von KI-Methoden bei der Polizei. Weitflächige Videoüberwachung zusammen mit automatischer Gesichtserkennung kann eingesetzt werden, um vermisste Personen zu finden oder Gefährder bei akuter Terrorgefahr zu verfolgen. Diese Anwendungen sind in der KI-Verordnung als Hoch-Risiko-Anwendungen eingestuft und sind unter strengen Bedingungen zugelassen. Einige Nichtregierungsorganisationen haben deshalb starke Bauchschmerzen, weil sie befürchten, dass die Anwendungen in der Zukunft ausgeweitet werden könnten, sobald ein umfassendes Überwachungssystem erst einmal im Einsatz ist.[13]

Im Film *Minority Report* arbeitet Tom Cruise in einer Pre-Crime-Einheit, die Verbrecher verhaftet, bevor sie ein Verbrechen begehen. Im Film wird das durch hellseherische Fähigkeiten möglich, die bei drei Richtern mittels Drogen induziert werden. Im normalen Polizeialltag

12 Aly & Roth (2000) beschreiben die Rolle von Statistik und maschineller Datenverarbeitung im Nationalsozialismus. Das Buch ist ursprünglich 1984 anlässlich der Diskussionen um die Volkszählung in der BRD erschienen.

13 Siehe Algorithm Watch (2024).

braucht es keine hellseherischen Fähigkeiten. Werden an bestimmten Orten immer wieder Verbrechen begangen, wird die Polizei dort mehr Präsenz zeigen, um Verbrechen zu verhindern. Big Data und Statistik versprechen allerdings Verbrechen genauer vorherzusagen. Bald wird es uns nicht mehr reichen zu wissen, dass in einem Stadtteil viele Verbrechen geschehen, wir werden auch wissen wollen, wer verdächtig ist. KI-Systeme können die Polizei dabei unterstützen, ihre Daten entsprechend zu analysieren. Wie im Film könnte man gezielt Personen identifizieren, die vielleicht Verbrechen begehen werden, um sie zu beobachten und zu kontrollieren. Das nennt man ›Predictive Policing‹. Auch hier gilt das DIDO-Prinzip (Zur Erinnerung: DIDO steht für ›discrimination in, discrimination out‹). Bedenken, dass der Einsatz von KI-Systemen Vorurteile und Rassismus verstärken und pseudowissenschaftlich begründen könnte, sind nicht rein akademisch. Die Polizei von Los Angeles hat solche Systeme ausprobiert und viele der Sorgen von Bürgerrechtlern haben sich leider bestätigt. Insbesondere führt jeder anlasslose Kontakt mit der Polizei dazu, dass es wahrscheinlicher wird, dass man wieder kontrolliert wird.[14]

Die Diskussion in Deutschland zum Einsatz von Big Data und KI bei der Polizei ist weniger aufgeheizt als in den Vereinigten Staaten. Wie in anderen deutschen Behörden sollen auch bei der Polizei Akten digitalisiert werden. Aber selbst wenn relevante Daten schon Digital zur Verfügung stehen, haben die Beamten nicht immer leicht Zugriff darauf. In Hessen gibt es daher das System hessenDATA, das Daten aus verschiedenen Quellen zur Analyse zusammenführen soll. In Bayern heißt das entsprechende System VeRA (Verfahrensübergreifende Recherche- und Analyseplattform) und in Nordrhein-Westfalen gibt es DAR (Datenbankübergreifende Analyse und Recherche). Gemeinsam ist diesen Systemen, dass unter der Haube die Software Gotham der amerikanischen Firma Palantir läuft. (Wer denkt sich diese Namen aus?[15]) Palantir beliefert auch Nachrichtendienste, deren Aufgabe es ist, möglichst viele Daten über alles und jeden zu sammeln. Ein Grund-

14 Der Einsatz von verschiedenen Systemen bei der Polizei von Los Angeles und die Folgen davon sind gut dokumentiert. Einen Überblick geben z.B. die Artikel von Haskins (2020), Bhuyian (2021) oder Hvistendahl (2021). Brayne (2021) hat den Einsatz von Big Data innerhalb der Polizei von Los Angeles in einer Feldstudie beobachtet und viele Interviews geführt. Siehe auch nochmal Katz (2020), Kapitel 4.

15 Gotham ist die verkommene Stadt aus den *Batman*-Comics und Palantir ist die alles sehende Kristallkugel aus Tolkiens *Der Herr der Ringe*. Ist Ihnen auch der Kontrast

prinzip des Datenschutzes ist allerdings, dass Daten normalerweise nicht für andere Zwecke eingesetzt werden dürfen, als für die sie gesammelt wurden. Das setzt dem Einsatz solcher Systeme enge Schranken. Das Bundesverfassungsgericht hat festgestellt, dass das hessische Gesetz zum Einsatz von hessenDATA verfassungswidrig ist und nachgebessert werden muss. Der bayerische Datenschutzbeauftragte hielt schon den Testbetrieb von VeRA für verfassungswidrig.[16]

Auf den ersten Blick scheint Deutschlands und Europas strenger Datenschutz die Entwicklung von KI hierzulande in allen Bereichen auszubremsen. Und tatsächlich hängt die Entwicklung von KI-Anwendungen mithilfe von Statistik und maschinellem Lernen ganz entscheidend vom Zugang zu großen Datenmengen ab. Weder China noch die Vereinigten Staaten messen dem Datenschutz – aus unterschiedlichen Gründen – im Vergleich zu Europa sehr viel Wert bei. China und die Vereinigten Staaten legen auch deshalb ein unglaubliches Entwicklungstempo vor, weil sie Datenschutzfragen oftmals einfach ignorieren. Auf den zweiten Blick ist daher durchaus Vorsicht geboten, wenn der Datenschutz leichtfertig aufgegeben werden soll, damit wir technologisch nicht abgehängt werden. Die rechtliche, politische und gesellschaftliche Diskussion muss daher mit den technologischen Entwicklungen Schritt halten.

Es entsteht manchmal der Eindruck, als ob KI eine vollkommen neue Technologie ist, die auf einmal über uns hereinbricht und auf die wir nicht vorbereitet sind. Das Sammeln von Daten und deren Verarbeitung mit statistischen und maschinellen Methoden ist aber nichts Neues. In vielen Bereichen, in denen KI-Methoden neuerdings eingesetzt werden, gibt es lange etablierte Regeln und Standards, die ebenso für KI gelten. Das Internet ist auch schon eine ganze Weile kein Neuland mehr. Dass die EU nach der Datenschutzgrundverordnung und den Gesetzen über digitale Märkte und Dienste nun eine KI-Verordnung verabschiedet hat, die viele aktuelle Entwicklungen aufnimmt, zeigt, dass es möglich ist, von den Entwicklungen nicht überrannt zu werden. Während ein Terminator-Szenario noch in den Bereich der Sci-

in der Namensgebung zwischen der amerikanischen Firma und den deutschen Behörden aufgefallen?

16 Zu hessenDATA und dem Urteil des Bundesverfassungsgerichts siehe Scheld (2023). Zu der Kontroverse um VeRA siehe Meyer-Fünffinger, Streule, Zierer, Kartheuser & Schöffel (2024).

ence-Fiction fällt, ist der Einsatz von KI-Methoden in einem digitalen Big-Brother-Szenario schon längst Realität und muss reguliert werden. Lassen wir uns nicht einreden, dass die Entwicklungen so schnell und überraschend sind, dass uns das nicht gelingen kann!