KULTUR NEU ENTDECKEN

SWR2

SWR2 Wissen: Aula

Lug und Trug im Internet

Die Mechanik der Täuschung

Von Marco Wehr

Sendung: Sonntag, 15. Dezember 2019, 8.30 Uhr
Redaktion: Ralf Caspary
Produktion: SWR 2019

In den Zeiten der Digital-Pioniere galt das Internet einmal als Ermöglichung weltweiter Transparenz, einer Welt ohne Grenzen. Und heute: Das sind nur noch Utopien, das Internet zeigt sein anderes Gesicht: Fakes, Datenklau, Manipulation, Cybergrooming. Meint Dr. Marco Wehr, Physiker, Philosoph, Autor und Gründer des Philosophischen Labors in Tübingen.

MANUSKRIPT

Anmoderation:

Mit dem Thema: „Lug und Trug im Internet – Die Mechanik der Täuschung“. Am Mikrofon: Ralf Caspary.

In den Zeiten der Digital-Pioniere galt das Internet einmal als Ermöglichung weltweiter Transparenz, Demokratie, einer Welt ohne Grenzen. Und heute: Das sind nur noch Utopien, das Internet zeigt sein anderes Gesicht. Da geht es um Fakes, um das Abgreifen von Daten, um das Manipulieren von Bildern.

Das meint jedenfalls Marco Wehr, Physiker, Philosoph, Autor und Gründer des Philosophischen Labors in Tübingen.

Marco Wehr:

Lug und Trug sind im Internet mittlerweile dermaßen verbreitet, dass man nicht genau weiß, wo man beginnen soll. Vielleicht beim Cybergrooming? Das ist eine Methode, mit der sich ältere Männer im Internet an junge Mädchen heranpirschen. Dazu legen sie einen sogenannten Fake-Account an. Sie verwenden ein falsches Profilbild und geben sich als junges Mädchen aus. Mit dieser “digitalen Maske“ treiben sie sich dann auf Foren herum, in denen sich Mädchen ihre Reiterlebnisse erzählen und ahnungslos Fotos von sich posten.

Meistens bleibt es bei voyeuristischen Betrachtungen. Aber leider nicht immer. So geschehen im schwäbischen Rottweil: Ein 38-jähriger Lastwagenfahrer diente sich einer 13-jährigen zuerst als gleichaltrige Freundin an, dann schmierte er ihr in einer anderen Rolle als 17-jähriger Casanova Honig ums Maul und gab sich zum Schluss als russischer Mafiakiller aus, der mit Mord und Totschlag drohte. Das maliziös inszenierte Ränkespiel überforderte das Mädchen, sodass es sich in seiner Verzweiflung tatsächlich mit ihm traf, worauf sie vom digitalen Puppenspieler vergewaltigt wurde. Der Täter wurde 2013 zu mehr als fünf Jahren Haft verurteilt.

Solche Extremereignisse sind zum Glück Ausnahmen. Nichtsdestotrotz hat sich das Prinzip des hinterlistigen Betrugs im Internet etabliert. Viel zu lange wurde nur dessen Transparenz in den Vordergrund gerückt, während man die Möglichkeit der Täuschung anfänglich nicht wahrnahm, sie dann nicht wahrhaben wollte, um jetzt endlich zu begreifen, dass da ein Ungeheuer von der Kette geht: Computerviren und Trojaner allerorten, dreiste Kapitalverbrechen mittels Phishing, dem Abgreifen vertraulicher Bankinformationen. Die Bedrohung durch skrupellose Hacker, die nicht davor zurückschrecken, Computersysteme in Krankenhäusern oder Kraftwerken außer Betrieb zu setzen, um Geld zu erpressen. Computertrolle, die das politische Klima vergiften. Und das ist noch nicht alles. Oft kommt die Hinterlist auf leisen Sohlen. Damit wären wir bei den Strategien vieler sozialer Medien.

Doch während die meisten Menschen Cybergrooming, das Hacken von Krankenhäusern oder den Diebstahl von Kontendaten moralisch verwerflich finden, verhalten sie sich vergleichsweise ahnungslos, wenn sie von Facebook&Co an der

Nase herumgeführt werden. Das ist die hohe Kunst der Täuschung. Denn diese verbreitete Arglosigkeit ist im Sinne der Betreiber. Deren Geschäftsmodell hängt schließlich davon ab, dass der Benutzer dessen Komplexität nicht durchschaut und deshalb auch nicht weiß, in welcher Weise mit ihm verfahren wird.

Um zu verstehen, wie die Verführungsstrategien von Firmen wie Facebook funktionieren, erinnern wir uns am besten an den Onkel, vor dem uns unsere Großeltern als Kinder immer gewarnt haben. Die undurchsichtige Gestalt verschenkt mit einem Lächeln im Gesicht Bonbons, obwohl sie nichts Gutes im Schilde führt.

In ähnlicher Weise setzt sich die Strategie von Social-Media-Plattformen wie Facebook häufig aus fünf elementaren Bausteinen zusammen: Zuerst wird der Nutzer gelockt. Dann macht man ihn gefügig. Das Entstehen von Abhängigkeiten ist im weiteren Verlauf nicht ausgeschlossen. Endlich greift man die ersehnten Daten ab, um sie zum Schluss zu versilbern.

Was ist das Lockmittel, mit dem ein Unternehmen wie Facebook arbeitet? Facebook stellt in Aussicht gleich ein Bündel grundlegender menschlicher Bedürfnisse zu befriedigen. Das Unternehmen wirbt damit, weltweit Freunde zu finden und mühelos seine sozialen Beziehungen pflegen zu können. Darüber hinaus fungiert die Plattform potenziell als Partnerportal. Außerdem ist sie hervorragend geeignet, sich selbst als Mensch in Szene zu setzen. Im Gegensatz zum wirklichen Leben, in dem sich Situationen oft ungeplant entwickeln, unterliegt die virtuelle Inszenierung der eigenen Kontrolle – ein unschätzbarer Vorteil im globalen Kampf um Aufmerksamkeit und Ansehen.

Da das Streben nach Ansehen gerade in unserer Zeit eine so fulminante Triebkraft ist, wollen wir es in Bezug auf die sozialen Medien kurz hinterfragen: Untersuchungen der Verhaltensbiologie belegen, dass Ansehen *ganz wörtlich* zu verstehen ist! Menschen mit hohem Ansehen werden von anderen Menschen im sozialen Miteinander tatsächlich mehr angesehen, während man Ausgestoßene keines Blickes würdigt! Die Gründe für großes Ansehen waren und sind kulturell allerdings verschieden.

In traditionellen Stammesgesellschaften konnte eine heilkundige Frau ein hohes Ansehen genießen oder ein erfolgreicher Jäger. In der Antike ein eloquenter Staatsmann, eine gelehrte Hetäre oder ein Philosoph. Und heute? Natürlich gibt es nach wie vor Menschen, die auf der Grundlage dessen, was sie können und leisten, geschätzt werden. Ansehen genießen aber auch viele nur deshalb, weil ihr Gesicht in den Medien allgegenwärtig ist. Der Trick, Bilder seines Antlitz‘ zu verbreiten, ist dabei nicht neu. Schon Alexander dem Großen war klar, dass er sein Ansehen vergrößern konnte, indem er massenhaft *Bilder* von sich selbst in Umlauf brachte. Dazu boten sich damals Münzen an, auf denen sein Konterfei zu sehen war.

Vor diesem Hintergrund versteht man, welche magnetische Wirkung die millionenfach verbreiteten Titelbilder des heutigen Boulevards und vor allen Dingen das Fernsehen auf Menschen mit histrionischen Persönlichkeitsmerkmalen ausüben. Der Drang, sich darzustellen und in Bild und Film überall gesehen zu werden, wird grenzenlos. Und wenn man guckt, wie Menschen im Dschungelcamp freiwillig glitschige Würmer vertilgen oder sich bei einer Castingshow von Dieter Bohlen

öffentlich zur Schnecke machen lassen, dann versteht man, dass eine zwanghafte Komponente im Spiel sein muss.

Trotzdem ist dieses vom Fernsehen zelebrierte und auch forcierte Spektakel nicht das Ende der Fahnenstange. Es wird durch das Internet getoppt. Jeder, der will, kann sich zum Regisseur seiner eigenen Person aufschwingen. Es genügt, millionenfach Likes, Freunde oder Follower zu generieren, um im Wettbewerb um Aufmerksamkeit und Ansehen oben mitzuschwimmen. Wie man das schafft, ist egal. Zwei halbwegs begabte Mädchen wie Lisa und Lena, die ihre Lippen rhythmisch zur Musik bewegen und dabei Grimassen schneiden, werden zu hofierten Idolen. Das ist die Proliferation des Banalen.

Wir halten fest: Die Möglichkeit, sich selbst in Text, Bild und Film nach eigenem Gusto zu inszenieren und seine Ich-Botschaften auf der ganzen Welt zu verbreiten, hat etwas ausgesprochen Verführerisches. Und dieser Köder wird von Facebook weidlich genutzt, auch wenn nicht jeder, der dieses Medium verwendet, sein Ego liftet.

Wie betont, es gehört zum Geschäftsmodell, dass der Genuss dieser “Annehmlichkeiten“ nichts kostet. Trotzdem ist nach der Preisgabe der persönlichen Daten ein weiteres kleines Opfer fällig: Der Benutzer muss bereit sein, sich maschinenlesbar zu machen. Da Maschinen nicht so klug sind wie Menschen, müssen *wir* uns freiwillig auf deren Niveau begeben, damit wir systemkompatibel und damit auslesbar werden.

Aber kommuniziert man auf Portalen wie Facebook nicht mit Menschen? Auch. Das Schnittstellendesign der Benutzeroberfläche ist aber alles andere als beliebig. Damit bei Facebook der Rubel rollt, muss gewährleistet sein, dass das *Klickverhalten* genau ausgelesen werden kann. Wann wird welches Bild oder welcher Link aktiviert und was folgt dann? Das sind Daten, die die nachgeschalteten Superrechner brauchen, damit aus eigentlich privaten Informationen prall gefüllte Bankkonten werden.

Und können in diesem Zusammenhang tatsächlich Abhängigkeiten entstehen? Das steht zu vermuten. Die offensichtlichste ist vielen bekannt: Bequemlichkeit macht unbeweglich. Grundlegende Fertigkeiten werden entweder gar nicht mehr gelernt oder verlernt. Wer es zum Beispiel gewohnt ist, alles, was er sucht, mit einem Navi zu finden, wird sich schwertun, wenn die Maschine nicht zur Hand ist. Und wer stundenlang potentielle Sexualpartner auf Tinder nach dem Wisch-und-weg-Verfahren selektiert, dem fehlt die geschmeidige Selbstverständlichkeit, auf der Straße spontan einen lockeren Spruch rauszuhauen.

Darüber hinaus ist es wahrscheinlich, dass echte psychische Abhängigkeiten entstehen können. Unser für Manipulationen empfindliches Dopaminsystem reagiert nämlich auf die *Erwartung* von Neuigkeiten – nicht auf die Neuigkeiten selbst. Dieser Umstand macht es erklärbar, dass einige Menschen den Eingang ihres Smartphones tausend Mal am Tag überprüfen. Und da sich außerdem viele Menschen über ihre sozialen Beziehungen definieren, kann man sich ausmalen, was es bedeutet, wenn in diesem sensiblen Bereich etwas schief läuft. Werden die realen Beziehungen auf

Kosten der virtuellen ausgedünnt, hat es gerade für Heranwachsende fatale Konsequenzen, wenn sie im Netz gemobbt und isoliert werden.

Nachdem nun der Kunde gelockt und gefügig gemacht wurde und nicht selten auch in Abhängigkeitsverhältnissen verstrickt ist, kommt für viele Anbieter sozialer Netze der ersehnte Moment: die Ernte. Die begehrten Daten müssen heimlich abgegriffen werden, damit sie sich anschließend zu Geld machen lassen. Um sich diesen Mechanismus zu verdeutlichen, hilft es, sich den Computerbildschirm wie eine Trennscheibe zwischen zwei völlig verschiedenen Welten vorzustellen.

Vor der Scheibe sitzt ein meist ahnungsloser Mensch, der mit Freunden herumblödelt, mit der Liebsten Geheimnisse austauscht, einen Film guckt oder auch mal eine Werbung checkt. Hinter der Scheibe sieht die Welt allerdings ganz anders aus. Hier treiben Computer- und Kognitionswissenschaftler sowie Statistikkoryphäen ihr Unwesen. Man darf sie sich guten Gewissens im weißen Laborkittel vorstellen. Ihnen geht es schließlich darum, das Nutzerverhalten wissenschaftlich zu erfassen. Die dem Benutzer abgewandte Seite ist deshalb so etwas wie ein ausgeklügelter Experimentalaufbau eines behavioristischen Psychologen. Die Behavioristen waren von der Idee beseelt, die Psychologie auf Reiz-Reaktions-Schemata zu reduzieren und ihr so das Gepräge einer harten Naturwissenschaft zu verpassen. Dazu müssen sich Input- und Outputdaten exakt kontrollieren und protokollieren lassen.

Sehr anschaulich wird diese verstörende Zweiweltentheorie bei Menschen, die ihre Bücher gerne auf einem Kindle von Amazon lesen. Selbst wenn sie scheinbar alleine mit einer Tasse Tee vor dem Kamin sitzen und schmökern, verfolgt sie der Konzern wie ein Schatten, zeichnet minutiös auf, wann Texte überflogen und wann sie sorgfältig studiert werden. Angeblich werden diese Informationen dazu verwendet, in Zukunft erfolgreichere Bücher zu konstruieren.

Für die Wissenschaftler von Facebook&Co ist also die Frage interessant, wie ein Nutzer, über den man im Laufe der Zeit immer mehr erfährt, reagiert, wenn er in einem bestimmten Augenblick ein fragliches Item, etwa eine Werbeanzeige auf dem Bildschirm, sieht. Klickt er, klickt er nicht? Wie lange bleibt er auf der Seite? Und wohin navigiert er dann? Diese wertvollen Datenspuren ergeben für unsere Forscher so etwas wie eine in der Zeit diskretisierte individuelle Verhaltenskinetik. Diese ist umso aussagekräftiger, je länger sich der Nutzer auf Facebook aufhält.

Und damit müssen wir kurz auf Mark Zuckerberg zu sprechen kommen, der nicht müde wird, dem Nutzer einen perfekt auf ihn zugeschnittenen Newsfeed zu versprechen.

Der Newsfeed ist so etwas wie das Herzstück vieler sozialer Netzwerke. Hier bekommt man Inhalte und sogenannten Status-Updates der anderen Nutzer zu sehen, außerdem wird man mit Nachrichten versorgt, die den eigenen Interessen entsprechen. Im ersten Moment klingt Zuckerbergs Versprechen unverfänglich. Aber die Motivation ist vermutlich nicht selbstlos. Eine bevorzugt an den eigenen Vorlieben orientierte Darstellung von Nachrichten, die man auch noch selbst durch Filtereinstellungen einengen kann, ist ein selbstbezügliches Optimierungssystem mit dem eigenen Ich als perspektivischem Fluchtpunkt. Deshalb gleicht ein personalisierter Feed von Nachrichten weniger einem Blick in die Welt, als vielmehr

einer ausdauernden Beschäftigung mit dem eigenen Spiegelbild. Die ohnehin schon beschränkte Echokammer schnurrt zur Egoblase zusammen. Wie es scheint, ist das vielen nicht unangenehm. Im Gegenteil. Und das ist im Sinne von Facebook, denn die Verweildauer auf der Seite wächst und damit das abschöpfbare Datenvolumen.

Es ist jetzt eine interessante, wenngleich schwierige Frage, welche Daten erhoben werden, wie sie ausgewertet, interpretiert, verwendet und verkauft werden. Geht es tatsächlich nur um personalisierte Werbung?

Zumindest der erste Teil der Frage, sollte sich klären lassen. Nach Paragraf 15 der Datenschutzverordnung muss jeder Nutzer seine Daten in Europa einsehen dürfen. Allerdings verhalten sich viele Konzerne bei Nachfragen wie ein nasses Stück Seife in der Badewanne. Am Anfang wird meist abgewiegelt: Man möge bitte den eigenen Verlauf checken. Hakt man allerdings nach, dann erhält man endlich den sogenannten *Clickstream*. Das ist sozusagen der umfassende Laborbericht, das digitale Gedächtnis. Jeder gedrückte Like-Button, alle aktivierten Links, jedes betrachtete Bild und jeder geschaute Film sind minutiös aufgeführt und alle Klicks lassen sich mit exakten Zeitangaben versehen. Dazu kommen die Seiten, die man vorher besucht hat, samt solcher die man danach anguckte. Alleine diese Datenfülle ist beeindruckend und leider auch verräterisch: Seit der Studie von Michael Kosinski von der University of Cambridge weiß man, wie *wenig* Information ausreicht, um teils intime Details über Menschen zu erschließen. Der Wissenschaftler zeigte das anhand der Verwendung des Like-Buttons. Nur durch die Analyse der Likes, die ein Nutzer verteilt, lässt sich mit recht großer Sicherheit sein Geschlecht und seine seine Hautfarbe ermitteln sowie seine sexuelle Präferenz und seine politischen Anschauungen.

Darüber hinaus drängt sich die Frage auf, ob die Analyse der Daten noch weitergehender sein könnte. Das Datenmaterial, das Konzerne wie Facebook en masse generieren, ist schließlich wie geschaffen für die forcierte Bearbeitung mit neuesten KI-Algorithmen, die eine Sache ganz herausragend können: Korrelationen ermitteln. Und in diesem Zusammenhang wird man nervös, wenn man an die letzten Facebookskandale denkt. Nach einer Recherche der New York Times soll Facebook ausgerechnet Firmen wie Google, Amazon, Microsoft und Spotify deutlich mehr Nutzerinformationen zur Verfügung gestellt haben, als bisher bekannt war. Auch passiert es immer wieder, dass zweifelhafte Firmen wie etwa Cambridge Analytica Zugriff auf Facebookkonten bekommen. Welche Korrelationen dann hinter hohen Mauern zu welchem Zweck abgeleitet werden, wird wohl bis auf weiteres das Geheimnis der Firmen bleiben, die mit diesen Daten arbeiten. Diese lassen sich nur ungern in die Karten blicken.

Vor diesem Hintergrund empfiehlt es sich für den kritischen Nutzer, genau darüber nachzudenken, für welche Zwecke er Computer und Smartphones gebrauchen möchte.

Wären damit alle Gefahren angesprochen, die im Internet auf uns lauern? Bei weitem nicht! Dunkle Wolken ziehen noch an anderen Stellen auf und verkünden Ungemach. Es geht um raffinierte Fälschungen und klandestine Durchleuchtung. Beginnen wir mit ersteren.

Obwohl es den meisten nicht bewusst ist: Viele bis dato für unverwechselbar gehaltene Persönlichkeitsmerkmale lassen sich schon heute in Bild und Ton eindrücklich imitieren. Das gilt zum Beispiel für die Stimme. Es reichen bereits 20 Minuten Sprachmaterial, das viele Menschen nichtsahnend im Netz verfügbar machen, damit ein Computer in der Lage ist, eine Stimme recht echt nachzuahmen. Mit Hilfe eines Programms wie VoCo von Adobe, wird jeder Satz, den man mit Tastatur eingibt, mit der Stimme wiedergegeben, die vorher gesampelt also aufgenommen wurde. Damit kann man jemanden Dinge sagen lassen, die er selbst nie sagen würde. Das kann unangenehme Konsequenzen haben. Was würde zum Beispiel passieren, wenn sich Pädophile diese Imitationsfähigkeiten des Computers zunutze machen und vermeintlich mit der Stimme der Eltern auf die Mailbox der Kinder sprechen? „Nicole, hier ist Mama. Komme bitte nach dem Reiten um 18 Uhr zu dem Parkplatz am Waldrand. Wir holen Dich ab.“ Auf dem Parkplatz warten aber nicht die Eltern, sondern der Verfasser der trügerischen Botschaft.

Und damit sind die Möglichkeiten des Betrugs nicht ausgeschöpft. Es ist Stand der Technik, auf der Grundlage von Filmaufnahmen genauestens zu analysieren, in welcher Weise bestimmte Menschen beim Sprechen Ihren Mund bewegen und mit welcher Mimik sie das tun. Und nach der Analyse folgt die Synthese. Im Resultat kann man eine Zielperson in einer computergenerierten Filmaufnahme jeden denkbaren Satz artikulieren lassen: mit ihrer persönlichen Stimme und Ihrer eigenen Mimik. Die Systeme werden in wenigen Jahren perfekt sein. Wer kann vor diesem Hintergrund noch entscheiden, was echt ist und was gefälscht wurde? Und was wird das in Zukunft für Konsequenzen haben? Eine Sache auf alle Fälle ist sicher: Authentifizierung wird im digitalen Lügenland zum Herrschaftswissen werden, denn hoch entwickelte digitale Analyseverfahren, mit denen sich der Schwindel aufdecken ließe, stehen dem Gros der Nutzer nicht zur Verfügung.

Diese verstörende Entwicklung hat sich seit längerem angekündigt, in den letzten Jahren aber unglaublich an Fahrt aufgenommen. Als analoge Fotos noch aufwendig in der Dunkelkammer entwickelt wurden, war viel handwerkliche Finesse notwendig, um ein Bild glaubwürdig zu manipulieren. Das gleiche galt für die früheren Zelluloid- und Polyesterfilme. Aus diesem Grund konnte man als Betrachter lange wenigstens einigermaßen sicher sein, dass das, was auf einem Foto oder im Film zu sehen war, auch tatsächlich so war. Doch schon 1994 konstatierte der Medienwissenschaftler William J. Mitchell, dass die Sicherheit, ein Foto dokumentiere die Wirklichkeit, unwiederbringlich vorbei war. Schon mit damaliger digitaler Technik gelang es, Fotos, auf denen Politiker zu sehen waren, so zu arrangieren, dass der Kontext der Beziehung zwischen den Personen völlig verändert wurde. Aber das war wenig im Vergleich zu gegenwärtigen Möglichkeiten. Im optisch-akustischen Bereich gibt es eigentlich nichts mehr, was sich nicht überzeugend fälschen ließe. Deshalb haben seit neuestem auch vertonte Filme als Dokumentation tatsächlichen Geschehens ausgedient.

Um nun das Thema der Durchleuchtung in den Blick zu nehmen, müssen wir die Perspektive ändern. Es gelingt nämlich nicht nur, Menschen ziemlich perfekt zu imitieren, sie lassen sich mit den passenden Werkzeugen auch präzise analysieren.

Betrachten wir zur Verdeutlichung eine ganz alltägliche Gesprächssituation. Der Inhalt der Worte ist nur ein kleiner Teil der Information, der zwischen Sprechenden

ausgetauscht wird. Viele andere wichtige Dinge schwingen in einer Unterhaltung mit: die Körperhaltung, der räumliche Abstand, das Minenspiel, Stimmlage und Betonung. Obwohl wir diese sublimen Informationen meist nicht bewusst wahrnehmen, sind sie wichtig, um das Gesagte richtig bewerten und einordnen zu können. Interessanterweise lassen sich sogenannte Deep Learning-Algorithmen so trainieren, dass sie in solchen Situationen viel genauer hinschauen können als Menschen und ihnen deshalb im feingewebten Spiel der Emotionen nichts entgeht. Natürlich verstehen die Computer die Gefühle nicht. Sie lesen aber deren Zeichen. Und das reicht *den Menschen*, die die Maschinen in ihrem Sinne ge- oder missbrauchen. Sie können mittels dieser Informationen auf die seelische Verfassung der observierten Menschen schließen. So lässt sich etwa das Minenspiel minutiös analysieren. Und Körpersprache und Gangbild zeigen, ob sie sich jemand unsicher fühlt oder in irgendeiner Weise auffällig macht.

Auch die Stimme gibt Geheimnisse preis. Sie verrät dem Computer zum Beispiel, ob der Observierte depressiv ist oder Gefahr läuft, an Parkinson zu erkranken. Und als wenn das nicht genug wäre, gibt es mittlerweile Firmen, die vorgeben, Probanden mittels analysierender Algorithmen umfassend charakterisieren und säuberlich in Schubladen einordnen zu können. Es gibt bereits große Unternehmen, die Software dieser Art verwenden, um Bewerber zu bewerten. Man kann sich leicht ausmalen, dass in Zukunft auch Headhunter Sprachdaten im Internet bei der Suche nach geeigneten Persönlichkeiten durchforsten. Es gibt Kritiker, die die Verlässlichkeit der Verfahren bemängeln. Andere, wie die Informatikerin Julia Hirschberg von der Columbia State University, halten die Bewertung der Persönlichkeit auf der Basis von Sprachdaten für seriöse Wissenschaft. Hirschberg selbst hat ein Programm entwickelt, das Lügner besser enttarnt als jeder Mensch. Was passiert, wenn ein solches Werkzeug im Sultanat Brunei in Verhören zur Anwendung kommt, um etwa die sexuelle Präferenz zu erfragen? Dort wurde damit gedroht, Homosexualität mit dem Tode zu bestrafen.

Wir sind als Gesellschaft also aufgefordert, klare Regeln setzen, sonst sind in naher Zukunft dystopische Szenarien denkbar.

Einen kleinen Vorgeschmack gab es bereits 2016, als in Russland die App *Find Face* auf den Markt kam. Mit dieser App lässt sich ein Foto eines Menschen seinem Profilbild in den sozialen Medien zuordnen. Bis vor kurzem war die App auf das russische Facebook-Pendant VK beschränkt. Das wird wohl nicht so bleiben. Für einen Stalker ist diese App nämlich eine Wunderwaffe: Eine unbekannte hübsche Frau auf der Straße erblickt, schnell ein heimliches Bild gemacht und schon lässt sich herauskriegen, wer sie ist, wenn sie mit Originalbild in den sozialen Medien aktiv ist. Das klingt noch einigermaßen harmlos. Aber es dauerte nicht lange, bis *Find Face* in einem anderen Kontext zur Anwendung kam. Man enttarnte Pornodarsteller und -darstellerinnen, um sie dann zu erpressen. Doch selbst damit sind mögliche Szenarien nur angerissen. Denken wir an dieser Stelle einmal alles zusammen und stellen uns exemplarisch die folgende Situation vor.

Ein Krimineller fotografiert einen unbescholtenen Bürger, der aus reiner Neugier das politische Programm einer radikalen Partei an einem Wahlstand durchblättert. Durch Abgleich mit Bildern im Internet ermittelt er dessen Identität. Da es dort auch Sprach- und Filmmaterial von ihm zu finden gibt, prüft er mittels beschriebener

Analyseverfahren, ob sein Opfer ängstlich ist und sich deshalb mit einiger Wahrscheinlichkeit erpressen ließe. Wenn dem so wäre, erstellt er ein Video mit Originalstimme und persönlicher Mimik, in dem der Fotografierte extremistische, menschenverachtende Parolen von sich gibt. Er stellt seinem Opfer nun Foto und Video zu, verbunden mit der Aufforderung 50.000 Euro auf ein anonymes Bitcoinkonto zu überweisen. Ansonsten droht er, das Machwerk viral zu verbreiten – mit unabsehbaren Folgen für den persönlichen Ruf des Adressaten.

Wollen wir eine solche Entwicklung? Auf alle Fälle sollte uns die Einschätzung von Artem Kukharenko, dem Chef-Entwickler von *Find Face*, in den Ohren klingen. In einem Interview sagt er, dass durch Software wie *Find Face* unsere Privatsphäre in großem Maße zerstört wird. Und bei dieser Feststellung machte er nicht den Eindruck als würde ihn das besonders beunruhigen.

Wer anders denkt und sich seine Privatsphäre zumindest in Maßen erhalten will, muss sich deshalb genau überlegen, was er von sich selbst und seinen Nächsten im Netz öffentlich macht. Vermutlich wäre es noch besser, direkt konsequent zu handeln: Um mögliche Manipulationen und Erpressungen auszuschließen, trifft man sich in der realen Welt mit vertrauten Menschen aus Fleisch und Blut und sorgt dafür, dass Handys und Computer ausbleiben. In diesem Sinne war der kürzlich verstorbene Karl Lagerfeld, der sowohl Handy als auch Uhr zeitlebens ablehnte, nicht ein aus der Zeit gefallener Hinterwäldler, sondern eher ein Visionär, der seiner Zeit voraus war. Die Zukunft liegt wohl im Altbewährten: dem persönlichen Gespräch von Angesicht zu Angesicht.

*****