Leseprobe

Eric Dolatre, Thilo Komma-Pöllath

Die notwendige Revolution

Er ist der Erfinder des Big-Data-Modells – und kämpft gegen die digitale Überwachungswirtschaft. Ein Insiderbericht

---

Bestellen Sie mit einem Klick für 22,00 €

Penguin Random House Verlagsgruppe | amazon.de | bücher.de | eBook.de
genialokal.de | Thalia | Hugendubel.de Das Lesen ist schön! | Weltbild.de

---

Seiten: 336

Erscheinungstermin: 01. März 2021

Mehr Informationen zum Buch gibt es auf

www.penguinrandomhouse.de

Inhalte

Zum Buch

Kaum einer kennt das Geschäft mit unseren Daten so gut wie er: Eric Dolatre ist einer der Gründer des erfolgreichsten europäischen Mailanbieters und Erfinder des datenbasierten Businessmodells von GMX, der »benutzerprofil-abhängigen Werbung«. Mit Sorge sieht er, wie aus Globalisierung und Digitalisierung eine weltweite Überwachungswirtschaft entstanden ist, die all unsere Lebensäußerungen in viel höherem Maße kontrolliert und steuert, als wir ahnen. Das Geschäft mit den Daten ist zum Geschäft mit den Menschen geworden, dem Missbrauch Tür und Tor geöffnet. Höchste Zeit, der Macht der Internetkonzerne Grenzen zu setzen, denn nicht alles, was ein Geschäft verspricht, darf auch ein Geschäft sein! Eric Dolatre plädiert für einen zivilen digitalen Ungehorsam, er fordert klare Regeln von der Politik – und als Unternehmer geht er die US-Giganten frontal an und setzt auf ein seriöses, sicheres Modell: eine verschlüsselte europäische Kommunikationsplattform, die wir heute nötiger brauchen denn je zuvor.

Der Report eines Insiders, der enthüllt, wie weit die Überwachung durch die Datenkonzerne bereits fortgeschritten ist – und der demokratischen Werten und Grundsätzen wieder zur Geltung verhilft.

ERIC DOLATRE
Die notwendige Revolution

Eric Dolatre
mit Thilo Komma-Pöllath

DIE NOTWENDIGE REVOLUTION

Er ist der Erfinder des Big-Data-Modells –
und kämpft gegen die digitale Überwachungs-
wirtschaft. Ein Insiderbericht

ARISTON

Bibliografische Information der Deutschen Bibliothek

Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen
Nationalbibliografie; detaillierte bibliografische Daten sind im Internet
unter http://dnb.de abrufbar.

Penguin Random House Verlagsgruppe FSC® N001967

Redaktion: Michael Schickerling
Umschlaggestaltung: Hauptmann & Kompanie Werbeagentur, Zürich,
unter Verwendung eines Fotos von © Random House / Kay Blaschke
Satz: Satzwerk Huber, Germering
Druck und Bindung: GGP Media GmbH, Pößneck
Printed in Germany

ISBN: 978-3-424-20221-2

»Es liegt in der menschlichen Natur,
vernünftig zu denken und unlogisch zu handeln.«
Anatole France

Inhalt

Kapitel 1

Digitale Evolutionstheorie: Wir werden dafür bezahlen müssen

Wenn man die Evolution als eine kontinuierliche Entwicklung begreift, die es dem Menschen ermöglicht, sein Leben auf der Erde immer noch ein Stück einfacher zu gestalten, dann haben wir gerade das Zeitalter der größtmöglichen Bequemlichkeit erreicht. Seine Spuren mögen rund dreihunderttausend Jahre zurückreichen, aber der Homo sapiens lebt nicht mehr in Erdlöchern und Höhlen, er trägt keinen Lendenschurz mehr, muss nicht mehr frieren und hungern, nicht mehr mit selbst gebauten Speeren auf die Jagd gehen und um sein tägliches Überleben fürchten.

Der Mensch 2021 gönnt sich den ultimativen Luxus, die ganze Zeit darüber nachdenken zu dürfen, wie er sich sein Leben noch ein Stück einfacher und bequemer gestalten kann. Der Mensch anno 2021 ist ein bisschen faul geworden. Er sitzt in seinem volldigitalisierten Smarthome und kann allein über Sprache und Gesten und, wer weiß, vielleicht auch schon bald mittels neurodigitaler Implantate über seine neurologische Verfasstheit, Gedanken und Gefühle sein alltägliches Leben steuern und organisieren. Im Gespräch mit einem »intelligenten« Lautsprecher erinnert ihn ein Computerprogramm daran, dass es Zeit wäre für seine Lieblingspizza von seinem Lieblingsitaliener. Was seine bevorzugte Pizza ist, das erkennt die intelligente Maschine auf Basis der Datenaufzeichnungen seiner Bestellhistorie von ganz allein. Der Algorithmus bestellt automatisch eine Cola dazu, weil er immer Cola trinkt. Wenn der Pizzabote zu Hause klin-

gelt, identifiziert die Gesichtserkennung der Überwachungskamera den Boten als den Boten seines Vertrauens, die Tür öffnet sich automatisch, und das Licht in der Küche und im Esszimmer geht an. Der Mensch 2021 zahlt ohne lästiges Bargeld, sondern nutzt Apple Pay, die 10 Prozent Trinkgeld sind voreingestellt und werden automatisch auf den Lieferpreis aufgeschlagen. Im Gespräch mit dem Lautsprecher erklärt er, dass er mit seiner Lieferung sehr zufrieden war, der ihm daraufhin anbietet, jetzt sein Lieblingslied von seiner Lieblingsband zu spielen, weil er immer Musik hört, wenn er isst. Etwas später wird der Algorithmus punktgenau die Standheizung seines Autos auf genau die Temperatur regeln, die er als angenehm empfindet, um entspannt und warm zu seinem voreingestellten Termin zu kommen. Für den Abend wird die künstliche Intelligenz das Herunterlassen der Jalousien auf genau die Zeit programmieren, zu der er gewöhnlich ins Bett geht. Nur essen und schlafen, das muss auch der Mensch 2021 noch selbst.

Ob wir hungrig oder müde sind, ob uns kalt ist oder warm, ob wir gesund oder krank sind, im digitalen Zeitalter weiß die Technologie, bevor es der Mensch weiß, was der zum Leben braucht. Da hat die Digitalisierung den tieferen Sinn der Evolution, dem Menschen das Leben immer noch ein bisschen einfacher, am besten so einfach wie möglich zu gestalten, konsequent zu Ende gedacht. Der Homo smart in seinem Smarthome muss heute nicht mehr aus der Höhle raus, um bei Wind und Wetter in archaischen Lebensbedingungen seine existenziellen Wünsche, Nöte, Sorgen und Gefahren zu befriedigen oder zu bekämpfen, er sitzt einfach nur da und sagt: »Alexa, eine Quattro Stagioni. Aber bitte schnell, ich habe Hunger!« Nicht selten fällt das »Bitte« auch noch weg, ist schließlich bequemer so.

Und wenn mein Verdauungsprozess einsetzt, nehme ich Platz auf meiner intelligenten Toilette, die in der Lage ist, meinen Urin und meine Exkremente zu analysieren und meine Gesundheit über einen lebenslangen Zeitraum zu überwachen. Die Mess-

daten der Toilette werden in meine Cloud übertragen, zu der der Gastroenterologe und Onkologe meines Vertrauens Zugang haben. Die smarte Toilette ist kein Schmäh, sie gibt es wirklich, Stanford-Forscher haben sie entwickelt für ein langes, gesundes und bequemes Leben. Gemeint ist wohl das ewige Leben.

Willkommen in der schönen, neuen Wirklichkeit! Noch Fragen?

Wir Arkoniden

Dass eine zu große Bequemlichkeit eine hoch entwickelte Spezies in den Untergang führen kann, wissen wir seit 1961. Es war das Jahr, als der erste *Perry-Rhodan*-Band erschien und auch in Deutschland von einem Millionenpublikum verschlungen wurde. Darin geht es um das größte Abenteuer der Menschheit: Major Perry Rhodan erlebt die fiktive Mondlandung acht Jahre vor Neil Armstrong. Er bruchlandet mit seinem amerikanischen Raumschiff auf dem Mond und entdeckt dort die Gesellschaft der Arkoniden, ein Volk menschenähnlicher Außerirdischer. Die Arkoniden halten sich für die Krone der Schöpfung, tatsächlich degenerieren sie zu apathischen, lethargischen, bequemen Geschöpfen, die nur noch vor ihren Monitoren sitzen und mit ihren Computern spielen, und alles andere wird unwichtig. Das öffentliche Leben kommt zum Erliegen, jeder Gemeinschaftssinn geht verloren, am Ende geht die Gesellschaft als Ganzes kaputt.

Liest man diesen ersten Band von Perry Rhodan von 1961, ist man mittendrin im Heute. Mit dem heutigen Wissen wirkt vieles gespenstisch. Im Zeitalter der neuen Weltreligionen Facebook, Twitter, WhatsApp und Instagram, im Zeitalter der neuen Bequemlichkeitsmaschinen Google, Amazon und Alexa, im Zeitalter von Fake News, Hatespeech und Dystopie, in denen immer mehr Menschen, auf der Suche nach dem Sinn, keinen

Sinn mehr finden können. Sind uns die Arkoniden Warnung genug?

Ich will gar nicht spöttisch klingen, auch wenn ich manchmal zum Zynismus neige. Ich selbst bin ein Vertreter der Computerei der ersten Stunde in Deutschland. Ich bin einer der vier Gründer von GMX, Ende der 1990er-Jahre einer der ersten großen E-Mail-Dienste der Welt. Wenn man sagt, dass GMX die digitale Kommunikation in Deutschland revolutioniert hat, ist das sicher nicht falsch. Ich war damals einer der Ersten, der die Idee in die Welt dachte, dass eine Computersoftware die Daten von Menschen sammeln und auswerten kann, um sie für Werbezwecke zu nutzen. Ich bin, wenn Sie so wollen und wie es im Fachjargon heißt, der Erfinder der benutzerprofilabhängigen Werbung. Es ist *das* Businessmodell der gesamten digitalen Welt von heute, das wir unter dem Schlagwort »Big Data« kennen – das Öl im Getriebe des 21. Jahrhunderts, so sagt man. Ich bin einer der Geburtshelfer der riesigen Digitalkonzerne von Facebook bis Google, die unser aller Leben so gefährlich einfach machen. Diese Konzerne werden unser Denken und unser Dasein in einer Radikalität verändern und bestimmen, die uns noch gar nicht ganz bewusst ist. Und gut möglich, dass wir es erst merken, wenn es zu spät ist. Das, was Big Data tatsächlich bedeutet, haben wir anno 2021 immer noch nicht begriffen.

Von den ersten Urmenschen und den Neandertalern über Perry Rhodan bis zu Alexa war es ein langer Weg, den eine immense technologische Entwicklung begleitet und erst möglich gemacht hat. Diese Entwicklung von der Höhle zum Smarthome ist eine Geschichte über den Menschen und seinen fast grenzenlosen Erfindergeist. Der menschliche Genius ist brillant, seine Neugier und sein Forscherdrang sind atemberaubend, fehlerfrei ist der Genius nicht.

Wer behauptet, wir lebten heute in einer perfekten Welt, weil sich alle so schön bequem darin einrichten können, hat vermutlich noch nie die Allgemeinen Geschäftsbedingungen der GA-

FAM-Konzerne im Wortlaut gelesen, den »Big Five« der weltweiten Online-, Computer- und Software-Industrie Google, Amazon, Facebook, Apple, Microsoft. Die Abkürzung GAFAM gibt es wirklich, und die Logik eines geschlossenen, höchst elitären Zirkels ergibt natürlich Sinn: Diese fünf amerikanischen Unternehmen sind die größten Influencer der Gegenwart, sie haben ein Beeinflussungsmonopol geschaffen, das einer freien Welt zuwiderläuft. Deren AGB zu lesen, das ist, entgegen des ursprünglichen Geschäftsgebarens der »Big Five«, auf einmal sehr kompliziert und aus gutem Grund äußerst unbequem. Auch deshalb wird ausgerechnet der »Geschäftsvertrag« zwischen den großen Digitalkonzernen und uns, ihren Usern, milliardenfach ungelesen weggeklickt, will sagen angenommen, was schon deshalb interessant ist, weil wir die Verträge, die wir im Allgemeinen, im realen Leben so abschließen – vom Autokauf bis zur Wahl unserer Haftpflichtversicherung –, im Detail kennen.

Das finnische IT-Sicherheitsunternehmen F-Secure hat sich vor sechs Jahren einmal den Spaß erlaubt, in die Nutzungsbedingungen eines öffentlichen Hotspots in London folgenden Satz hineinzuschreiben: »Mit der Benutzung dieses Dienstes willigen Sie ein, Ihr erstgeborenes Kind zu überlassen. Zeitpunkt und Nutzungsart werden vom Unternehmen festgelegt. Falls keine Kinder produziert werden, wird stattdessen Ihr Haustier genommen. Diese Bestimmungen gelten für die Ewigkeit.« Was glauben Sie, wie viele Nutzer diese Geschäftsbestimmungen bestätigt haben? F-Secure beeilte sich danach mitzuteilen, die Klausel, obwohl sie laut Rechtsberatern bindend war, nicht durchsetzen zu wollen. Der Verkauf von Kindern gegen Gratisdienste sei vor Gericht wohl nicht durchsetzbar, erklärten Juristen. Ganz sicher waren sie sich nicht. Trotz der, wenn auch kurzen, weltweiten Aufmerksamkeit für diese spektakuläre Aktion hat sich an der mangelnden Lektüre von AGBs bis heute nichts geändert.

Für die großen Digitalkonzerne ist es noch viel bequemer, seit wir es gerne so bequem wie möglich haben wollen. Wer also be-

hauptet, die digitale Welt sei eine perfekte Welt, hat vermutlich einmal zu oft weggeklickt, hat nie die Gesetzesnovelle des amerikanischen Cloud-Acts gelesen. (Kennen Sie den Cloud-Act überhaupt? Sollten Sie unbedingt!) Dem sagen Firmen wie DoubleClick oder Qualcomm nichts, der hat sich nie gefragt, warum es in der ganzen Welt nur ein Microsoft-Office-Programm gibt, aber so viele, unterschiedliche Arten von Cookies, die trotz ihres niedlichen Namens ein so monströses Beschattungswerk verrichten. Der weiß nicht, zu was WeChat imstande ist, was Oracle im Geheimen tut, in welche Welt wir eintreten, wenn 5G der Standard und das Internet der Dinge Wirklichkeit werden. Mit einem Satz: Wer das sagt, der irrt gewaltig!

Damals, Ende der 1990er-Jahre, war das alles noch nicht absehbar. Wir alle waren wie im Rausch ob der Möglichkeiten, Raum und Zeit ein Schnippchen zu schlagen. Die Idee vom »Global Message eXchange«, wie GMX ausgeschrieben heißt, also davon, einen elektronischen Brief in Echtzeit verschicken und mit der ganzen Welt kommunizieren zu können, das war in jenen Jahren des digitalen Eisprungs ein Freiheitsversprechen wie der erste Rausch, der erste Sex oder das erste eigene Auto, als die Straßen noch frei waren und niemand von Greta und dem Klimawandel sprach, von einem Corona-Lockdown ganz zu schweigen. Außer GMX kannte dieses Versprechen noch der amerikanische Dienst Hotmail, der etwa ein Jahr vor uns an den Start ging, das war es aber auch. Fragt man hierzulande die Menschen in der U-Bahn, in der Fußgängerzone oder im Supermarkt in einer Spontanumfrage nach ihrer ersten E-Mail-Adresse, sagen die allermeisten: GMX.

Was seit der Erfindung des Computers 1941 durch den deutschen Tüftler Konrad Zuse und seit der Erfindung des Internets 1969 durch das Pentagon und die beiden kalifornischen Universitäten in Berkeley und Stanford und schließlich seit der Etablierung einer digitalen Parallel- und Gegenwelt durch die Silicon-Valley-Konzerne in den letzten zehn Jahren im Überschalltempo voran-

getrieben wurde, ist eine Revolution, die nur mit der Erfindung der Elektrizität oder der Kernspaltung zu vergleichen ist. Nicht mehr lange und die datenvernetzte Welt, das Internet der Dinge, wird als die größte Erfindung in der Geschichte der Menschheit gelten. Daran kann heute kaum noch ein Zweifel bestehen.

Demokratie in Gefahr

Mindestens genauso wahrscheinlich, obwohl es sich die wenigsten vorstellen können, ist aber auch, dass wir eine Überwachungs- und Manipulationsmaschinerie in Gang gebracht haben, die sich kontinuierlich verselbstständigt und die der Mensch irgendwann nicht mehr stoppen kann. Eine intelligente Maschinerie, wie sie James Cameron 1984 im ersten *Terminator*-Film mit »Cyberdyne« visionär vorausgedacht hat: ein IT-Konglomerat, das mithilfe der künstlichen Intelligenz neuronale Prozessoren entwickelt, um *alle* Datenströme zu überwachen, also die Datenströme und Smartphones von allen. 1984 hat man als Nicht-Science-Fiction-Fan vielleicht noch über die Story des Films geschmunzelt. Bei Camerons Fortsetzung von 2019 läuft es einem schaurig über den Rücken. Die Realität hat die Fiktion schon lange eingeholt und überholt.

Dass ausgerechnet mein Geschäftsmodell zwanzig Jahre später eine kollektive Gier nach Daten losgetreten hat, mit der riesige Digitalkonzerne heute Milliarden US-Dollar umsetzen, betrifft mich insofern auch ganz persönlich. Eine Gier, die heute das tut, was wir Gründer von GMX ethisch und moralisch immer abgelehnt haben: E-Mails, Chats, Posts, Tweets mitzulesen, als gäbe es kein Post- und Fernmeldegeheimnis, Nutzer- und Nutzungsverhalten auszuspähen wie ein legaler Geheimdienst. Und alles nur aus sehr profanen Beweggründen: um noch genauer Werbung verkaufen und immer noch mehr Geld verdienen zu können.

Nicht nur die großen Digitalkonzerne, auch die alteingesessenen, analog produzierenden DAX-Unternehmen, Autobauer, Fluggesellschaften, Versicherer, Großhändler, Sportartikel-, Pharma- oder Zementfirmen überlegen fieberhaft, wie sie zusätzlich datenbasierte Geschäftsmodelle aus ihrer analogen Produktpalette heraus monetarisieren können. Es ist ein weltweiter Hyperwettbewerb um unsere persönlichsten Daten entbrannt, dem Grund- und Menschenrechte wie die Unverletzlichkeit der Wohnung, unsere Intim- und Privatsphäre im Zweifel herzlich schnuppe sind. Einen solchen Wettbewerb hat es nie zuvor gegeben. Nicht Menschen, sondern komplexe Computerprogramme sammeln, verifizieren und verbinden alle Spuren, die wir im Netz hinterlassen, schneller und umfassender denn je. Das ist die totalitäre Transparenz, die man keinesfalls mit totaler Freiheit verwechseln sollte. In der Totalität ist für den Einzelnen selbst die Freiheit ein Gefängnis.

Welche Rohdaten genau von uns gesammelt und gespeichert werden, welche Daten von uns aus unterschiedlichen digitalen Quellen und Kanälen zusammengeführt, miteinander verknüpft und extrapoliert, das heißt, analysiert werden, das wissen wir nicht. Die Algorithmen, die unsere Daten auslesen, kennen wir nicht. Alles Geschäftsgeheimnisse von GAFAM und Co. Es gibt natürlich noch viel mehr als die fünf großen US-Multis, auch solche, denen Demokratie nicht nur aus Geschäftsgründen, sondern schon kulturell suspekt ist. Ein Blick nach China reicht dafür völlig. Die Monetarisierung von Big Data ist der dunkle, wenig smarte Teil dieses ach so smarten Geschäftsmodells. Der unsichtbar im Hintergrund ablaufende Handel mit den kostenlosen und gerade deshalb sehr kostbaren Daten von Milliarden aktiven und nichtaktiven Nutzern, mutmaßlich einem großen Teil der Weltbevölkerung, durch einige wenige Datenkonzerne, wird unsere Gesellschaft in einer Art und Weise beschädigen, die jetzt noch gar nicht abschätzbar ist. Und es sieht ganz so aus, als würden diese Handvoll Konzerne in Darwins Evolutionstheorie

die perfekte Systematik für ihr perfides Geschäftsmodell finden. »Survival of the fittest« heißt im digitalen Zeitalter: Diejenigen, die es nur bequem haben wollen, wir Nutzer also, werden nicht stark genug sein, um sich gegen die Datenkraken wehren zu können, die in einer digitalen Zukunft keine natürlichen Feinde mehr fürchten müssen.

Schon heute gibt es digitale Superkonzerne, die mächtiger scheinen als die Regierungen oder Staaten, von denen sie eigentlich kontrolliert werden sollten. Als Facebook-Chef Mark Zuckerberg 2018 vor dem EU-Parlament zum Datenschutz seines Unternehmens Stellung beziehen sollte, war die Ehrfurcht der Parlamentarier vor dem großen Zuckerberg raumgreifend. Seine Erkenntnisse zum bisher größten Datenskandal überhaupt – den britischen Analysedienst Cambridge Analytica betreffend, der 2016 ungehindert auf Daten von 87 Millionen Facebook-Nutzern zugreifen konnte, um sie etwa für Donald Trump und dessen Präsidentschaftswahlkampf aufzubereiten – waren es eher nicht. Als Zuckerberg im Oktober 2019 vor dem US-Kongress noch einmal dazu befragt wurde, wann er denn von dem Skandal, der zu dem Zeitpunkt bereits drei Jahre zurücklag, eigentlich erfahren habe, antwortete er wörtlich: »I don't know!« Was sagt uns das, wenn er es nicht weiß oder nicht wissen will oder vorgibt, es nicht zu wissen? Außer einer peinlichen Stille blieb sein Auftritt ohne weitere erkennbare Konsequenzen. Wieso kommt Zuckerberg damit durch? Ist Facebook schon zu groß, um noch ernsthaft kontrolliert werden zu können? Too big to fail? Haben Trump und Zuckerberg womöglich eine ganz ähnliche Agenda, die lautet: Daten sind Wissen und Wissen ist Macht!

Was heißt das für eine demokratische Gesellschaft, wenn wenige fast alles über alle anderen wissen? Vor allem, wenn die wenigen gar nicht demokratisch legitimiert sind, sondern kommerziell motiviert? Darf man den Datenschutz von Millionen in einer Demokratie überhaupt privatisieren? Und was, wenn

diese Informationen in falsche Hände geraten, mit bösen Absichten? Dabei gibt es in Europa die Datenschutz-Grundverordnung, kurz DSGVO, die mich auf meinem Weg durch das Internet schützen soll. Aber wie ist es dann möglich, dass ich die Autonomie und das Urheberrecht an meinen Daten nicht habe und an einen Unternehmer wie Mark Zuckerberg abtreten muss – also den Daten, die so nur ich hinterlasse, die so auch nur mich persönlich identifizieren? Warum liegt der Schutz der Bürger durch Polizei und Sicherheitsbehörden aus gutem Grund in öffentlicher Hand, der Schutz der Daten der Bürger aber in privater? Und was machen so unfassbar viele Daten mit freiheitlichen, ethischen und kulturellen Errungenschaften? Steht der supranationale Algorithmus über jeder nationalen Verfassung? Was passiert, wenn das freie Spiel der Kräfte im Kapitalismus diese Daten zum Pfand macht für Demokratie und Freiheit? Liebe Leser, ich frage Sie: Warum vertrauen wir einem amerikanischen Konzern mehr als unserem eigenen Rechtsstaat? Und warum stört uns das alles nicht?

Das Datenschutzparadoxon

Wie bei allen großen, umwälzenden Innovationen treten irgendwann Risiken und Nebenwirkungen auf, die auf keinem Beipackzettel notiert sind. Ob bei der Atomkraft, Röntgenstrahlen oder FCKW in den Kühlschränken: Ich habe die Befürchtung, wir Menschen sind nicht besonders gut im Umgang mit solchen Nebenwirkungen, insbesondere, wenn wir sie mit unseren körperlichen Sinnen nicht wahrnehmen können.

Natürlich dürfen negative Begleiterscheinungen keine Innovationsbremse sein. Gerade die westliche Welt, insbesondere eine Industrienation wie Deutschland, das Label »Made in Germany«, lebt von seiner Innovationskraft – man denke nur an den viel gerühmten deutschen Mittelstand. Aber statt Neben-

wirkungen rasch zu analysieren und zu beseitigen, schauen wir ihnen lange beim Danebenwirken zu und tun nichts. In der Zwickmühle aus dem, was technisch möglich, und dem, was gesellschaftlich geboten ist, verfällt der Mensch gerne in eine paradoxe Starre: Wir lassen es laufen, obwohl wir wissen, dass wir längst einschreiten müssten. Wir befinden uns erst am Anfang einer Periode gewaltiger Umbrüche. Vieles, was meine Generation in den letzten fünfzig Jahren angerichtet hat, werden wir selbst nicht mehr richten können.

Am Klimawandel sieht man das am deutlichsten: Die Erfindung des Automobils durch Carl Benz gegen Ende des 19. Jahrhunderts war einmal ein großer zivilisatorischer Schritt. Aber schon sehr lange wissen wir, welchen Schaden Abermillionen Autos auf unserem Planeten und an unserer Atmosphäre anrichten. Und obwohl der Klimawandel, und was wir gegen ihn tun müssen, das gesellschaftliche Thema schlechthin ist, waren noch nie so viele, so große und so umweltschädliche Fahrzeuge auf unseren Straßen unterwegs: 2019 waren das erste Mal über eine Million SUVs und Geländewagen zugelassen – deutscher Rekord! Und schlimmer als Autos sind Flugzeuge und Kreuzfahrtschiffe – vor Beginn der Coronapandemie sind noch nie so viele Menschen geflogen oder mit einem Luxusdampfer in den Urlaub gefahren. Die weltweite Massentierhaltung, die mit ihrem CO_2-Ausstoß nicht nur die Atmosphäre zerstört, sondern den Regenwald gleich mit – noch nie gab es so viel Billigfleisch wie heute. Fragt man die Verbraucher, schwärmen sie von qualitativ hochwertigen, regionalen Lebensmitteln – tatsächlich geht die überwiegende Mehrheit beim Discounter einkaufen. Wie passt das alles zusammen? Der Mensch ist ein paradoxes Wesen, im Umgang mit den digitalen Verführbarkeiten noch einmal in besonderem Maße.

Wenn ich mit Menschen ins Gespräch komme über ihren digitalen Alltag, also konkret, den Umgang mit ihrem Smartphone – und das passiert ziemlich häufig, weil ich sie ununter-

brochen anspreche und danach frage –, höre ich vor allem zwei Sätze. Der erste Satz lautet: »Ich habe ja nichts zu verbergen!« Und der zweite: »Wer interessiert sich schon für mich und meine Daten?« Beide Antworten sind, ganz objektiv betrachtet, natürlich falsch: Jeder hat etwas zu verbergen, denn ohne Privatsphäre gibt es in einer freien Welt keine Individualität und keine Freiheit. Und im Gegenzug gibt es zu viele, die sich sehr stark gerade für mich interessieren, wenn auch nicht um meiner selbst willen.

Immer wieder versuche ich, ausführlich zu erklären, was Facebook und Co. mit den sogenannten »personenbezogenen Daten« dieses oder jenes Nutzers anstellt, wie diese Daten gespeichert, gesammelt, ausgewertet, hin- und hergeschoben und verkauft werden. Auch, wie gefährlich es doch wäre, wenn diese sehr persönlichen Informationen in die falschen Hände gerieten. Und dass man diese Daten sicher nicht seinem Nachbarn, nicht der Polizei und schon gar keinem Fremden an seiner Haustür einfach so übergeben würde, aber offensichtlich kein Problem damit hat, sie an ein amerikanisches Privatunternehmen mit Sitz im kalifornischen Palo Alto weiterzugeben, von dem man keinen einzigen Mitarbeiter persönlich kennt. In neun von zehn Fällen höre ich dann diesen oder einen ähnlichen Satz, der plötzlich ganz anders klingt: »Ups, Sie haben völlig recht. Darüber habe ich mir so konkret noch gar keine Gedanken gemacht!« Das »Datenschutzparadoxon«, so nenne ich das, besteht darin, dass mutmaßlich zehn von zehn von mir Befragten an ihrem Nutzerverhalten auch am nächsten Tag nichts ändern werden. Wie lässt sich das erklären? Und warum eigentlich nicht? Was hält uns davon ab?

Dass wir von alldem nichts gewusst haben oder nichts haben wissen können, kann niemand behaupten. Und man muss nicht einmal mir persönlich begegnet sein, um Aufklärung zu bekommen. Buchstäblich jeden Tag schwappen neue Datenlecks und Datenhacks und Datenskandale zu uns herüber, dazu zahllose

Berichte von Sicherheitsexperten und Datenschützern. Es gibt also die, die uns warnen wollen, und es gibt uns, die wir den miesepetrigen, vermeintlich zukunftsfeindlichen Spielverderbern mit der ewig gleichen paradoxen Nonchalance begegnen und alle Warnungen vor Sicherheitsrisiken in den Wind schießen.

Hier eine kleine Auswahl an Nachrichten, die während der Recherche zu diesem Buch erschienen sind, einfach nur in chronologischer Ordnung. Nachrichten, die die gesamte Bandbreite aller möglichen Sicherheitsrisiken abdecken, vom Systemfehler bis zu Spionage, von gewollten Hacks bis zu zufälligen Lecks, von wissenschaftlichen Studien bis zu politischer Willkür, von profanem Missbrauch bis zu gnadenloser Unterwerfung, von Marktversagen bis zu digitalem Hyperwachstum. Nachrichten, die es wieder nicht geschafft haben, unsere Aufmerksamkeit zu bekommen, um unser Verhalten zu verändern:

28. Oktober 2020: Unbekannte haben die Wahlkampfseite von US-Präsident Donald Trump gehackt. Auf der Seite prangten die Logos der amerikanischen Bundespolizei FBI und des US-Justizministeriums. Dazu hieß es: »Diese Seite wurde beschlagnahmt. Die Welt hat genug von den Fake News, die täglich von Donald J. Trump verbreitet werden.« Die Hacker verlangten für kompromittierende Enthüllungen über Trump die Einzahlung von Kryptowährung.

27. Oktober 2020: Cyberkriminelle haben in Finnland Daten von Zehntausenden Patienten erbeutet. Die vertraulichen Informationen stammen aus Therapiesitzungen des privaten Psychotherapiezentrums Vastaamo. Etliche Patienten berichten, dass sie von den Hackern erpresst worden seien, 200 Euro in Bitcoin zu überweisen, damit ihre Krankenakten nicht veröffentlicht würden.

22. Oktober 2020: Der Geheimdienstausschuss des US-Senats kommt in einer Untersuchung zu dem Schluss, dass Iran und Russland Einfluss auf den Ausgang der Präsidentschaftswahl am

3. November nehmen wollen. Beide Länder hätten persönliche Daten registrierter Wähler erbeutet und würden gezielt Falschinformationen verbreiten, so Geheimdienstkoordinator John Ratcliffe. Ziel dieser Wahleinmischung sei es, »Verwirrung zu stiften, Chaos zu säen und das Vertrauen in die amerikanische Demokratie zu untergraben«. Bereits 2016 hatte Russland durch Hackerangriffe und Internetkampagnen mit falschen Identitäten, sogenannten Trolls, den Ausgang der Präsidentschaftswahl massiv zugunsten von Donald Trump beeinflusst.

15. Oktober 2020: Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat darauf hingewiesen, dass in Deutschland 40.000 Unternehmen eine Sicherheitslücke auf ihrem Exchange-Server haben. Die Lücke sei seit Februar bekannt und noch immer nicht geschlossen worden, offensichtlich würden sich die Administratoren nicht um die Sicherheit der Firmensysteme kümmern. Der Exchange-Server ist die Kommunikationszentrale der Unternehmen, über die E-Mails, Kontakte und Kalendereinträge abgewickelt werden. Über ein aus dem Internet erreichbares Web-Interface sei es möglich, das System durch diese Lücke komplett zu übernehmen, heißt es. Das BSI nennt die Bedrohungslage »geschäftskritisch«, auch weil Hacker über den Server schnell in den Besitz von Administratorenrechten gelangen könnten.

18. September 2020: Nach einem Cyberangriff auf die Einwanderungsbehörde Argentiniens haben Hacker einen Datensatz mit sensiblen Passdaten von 12.000 deutschen Touristen ins Netz gestellt, darunter auch ranghohe Diplomaten. Insgesamt handelt es sich um Daten von Hunderttausenden Reisenden aus mehreren Ländern, die gestohlen wurden. Die Hacker hatten die Daten erst verschlüsselt und dann ein Lösegeld für die Entschlüsselung gefordert. Als die Behörde nicht zahlte, wurde eine zwei Gigabyte große Datei im Internet hochgeladen. Verbraucherschützer warnen davor, dass Cyberkriminelle die Daten für einen Identitätsdiebstahl nutzen und damit Fake Shops und Konten bei Onlinebanken eröffnen könnten.

28. August 2020: Der amerikanische Autobauer Tesla war Ziel einer Cyberattacke, bestätigte Tesla-Chef Elon Musk. Danach soll ein Russe versucht haben, einen Tesla-Mitarbeiter zu bestechen, Schadsoftware in die IT-Systeme der Firma einzuspeisen. Sein Plan war es, Daten zu stehlen und das Unternehmen damit zu erpressen. Der Plan ging schief, weil sich der Mitarbeiter als loyal erwies und das FBI informierte. Musk sprach von einem »ernst zu nehmenden Angriff«.

20. August 2020: Der Chauffeurdienst des Deutschen Bundestags wurde mit einer Erpressersoftware angegriffen. Die IT-Verwaltung des Bundestags teilte mit, dass keine sensiblen Daten abgegriffen wurden. Mit den richtigen Daten könnten Hacker Privatadressen, Bewegungsmuster und Treffen von Parlamentariern ausspähen. Kritik gibt es an den langen Speicherfristen von drei Monaten zu jedem einzelnen Fahrauftrag des BwFuhrparkService. Wer hinter dem bei Cyberkriminellen beliebten Erpressungstrojaner Emotet steckt, der meist mit einer infizierten Fake-E-Mail eingeschleust wird, ist bis heute unbekannt. IT-Experten vermuten die Hintermänner in Osteuropa. Auffällig ist, dass es in Russland fast nie zu Emotet-Infektionen kommt.

13. August 2020: Experten des IT-Sicherheitsunternehmens Check Point berichten von neuen Sicherheitslücken bei Amazons Smartspeaker »Echo«. Hacker könnten durch die Schwachstelle Wohnadressen, Telefonnummern, Bankdaten ausspähen und sogar Gespräche belauschen. Amazon bestätigte, dass man die Lücke nach Bekanntwerden umgehend geschlossen habe. Weltweit wurden mehr als 100 Millionen Echo-Lautsprecher verkauft.

7. August 2020: Auf der IT-Sicherheitskonferenz Black Hat haben IT-Forscher den Beweis dafür angetreten, dass es 18 verschiedene Wege gibt, den Absender einer E-Mail zu fälschen. Getestet wurden zehn der bekanntesten E-Mail-Anbieter und 19 populäre E-Mail-Programme, die allesamt ausgetrickst werden konnten. Forscher der Universität Berkeley konnten nach-

weisen, dass man E-Mails bei allen Programmen so aussehen lassen kann, dass sie von legitimen Adressen kommen, und die Prüfmechanismen des im Internet üblichen E-Mail-Protokolls SMTP in die Irre geführt und umgangen werden.

6. August 2020: Deutsche und italienische Sicherheitsforscher haben Schwachstellen in WLAN und Bluetooth-Chips entdeckt, die mehr als eine Milliarde Geräte weltweit betreffen. Laut den Forschern könnten Hacker, die sich in der Reichweite eines Bluetooth-Signals befinden, das WLAN-Signal ihrer Opfer ausschalten und dafür sorgen, dass die angegriffenen Geräte abstürzen. Sogar eine Schadsoftware kann über einen Bluetooth-Angriff aufgespielt werden. Betroffen sind unter anderem die neuesten iPhones ab Modell 6, alle Apple Watches und Laptops wie das MacBook und nahezu alle Samsung-Smartphones.

21. Juli 2020: Nach Recherchen von WDR und BR ist das Bundeskriminalamt (BKA) schon seit Jahren in der Lage, Messenger-Dienste wie WhatsApp zu überwachen. Das BKA-Referat »Informationstechnische Überwachung« habe einen Weg gefunden, an verschlüsselte Chats zu kommen, heißt es in einem internen Schreiben. Offenbar nutzen die Ermittler die Möglichkeit, WhatsApp über den Webbrowser zu steuern. Für des BKA handelt es sich beim Mitlesen von »WhatsApp Web« um eine reguläre Telekommunikationsüberwachung, schreiben die Datenjournalisten. Bisher hieß es, eine Überwachung der Kommunikation über Ende-zu-Ende-verschlüsselte Messenger-Dienste sei nicht möglich.

16. Juli 2020: Bei einem Twitter-Hack wurden die Accounts von rund 130 meist prominenten Persönlichkeiten gekapert. Darunter Elon Musk, Bill Gates, Barack Obama, Joe Biden oder der offizielle Apple-Account. Über die Profile wurde Werbung für eine dubiose Kryptowährung verbreitet. Offenbar konnten die Hacker auch die persönlichen Nachrichten der jeweiligen Nutzer lesen. Da der Angriff über ein internes Twitter-Programm geschah, geht das FBI davon aus, dass ein Twitter-Mitarbeiter

den Hackern geholfen hat. Da Twitter im August 2019 schon einmal gehackt wurde, damals war es der persönliche Account von Twitter-Chef Jack Dorsey, lässt der neuerliche Hack die Sicherheitsvorkehrungen des Unternehmens ziemlich blamiert dastehen.

22. Juni 2020: Die Aktivisten des Kollektivs Distributed Denial of Secrets (DDoS) haben Hunderttausende interne Dokumente von verschiedenen US-Polizeibehörden im Netz veröffentlicht. Die Datensammlung aus 24 Jahren umfasst 269 Gigabyte und ist online durchsuchbar. Die Unterlagen beinhalten Namen, E-Mail-Adressen, E-Mails, Telefonnummern, Fotos, Videos, PDF-, ZIP- und CSV-Dateien. Auch das FBI ist betroffen. Experten gehen davon aus, dass die Unterlagen Hinweise zu Informanten und verdeckten Ermittlern liefern und Kriminelle einen großen Nutzen aus den Daten ziehen können. Wie DDoS an die Dokumente gelangt ist, ist unklar. Möglicherweise wurde ein Dienstleister der Polizeibehörden gehackt.

17. Juni 2020: In einem Brief an den Geheimdienstkoordinator John Ratcliffe zeigt sich der demokratische Senator Ron Wyden besorgt über die IT-Sicherheit der US-Geheimdienste. Im Anhang des Briefs befinden sich Auszüge eines internen CIA-Berichts von 2017. Darin heißt es, dass ein CIA-Mitarbeiter im Frühjahr 2016 bis zu 34 Terabyte Daten gestohlen habe, das entspräche etwa 2,2 Milliarden DIN-A4-Seiten. Bemerkt wurde der Diebstahl erst ein Jahr später.

3. Juni 2020: Dank Corona hat der US-Videochatanbieter Zoom seinen Umsatz verdoppelt und rechnet mit einem Jahresergebnis von 1,8 Milliarden Dollar. Auch in Deutschland gibt es einen Zoom-Boom. Unternehmen, Behörden, Universitäten und Schulen nutzen die App für Besprechungen, Unterricht oder geheime Sitzungen, obwohl es immer wieder Kritik an den Sicherheitslücken gibt. Im April wurde eine Gedenkveranstaltung der Israelitischen Botschaft Berlin mit Pornos und Hitlerbildern gestört, im Mai wurde der Zoom-Unterricht einer Ham-

burger Gymnasialklasse mit einem eingeblendeten Hakenkreuz torpediert, in anderen Fällen wurde Kinderpornografie eingespielt. In 16 Fällen ermittelt die Polizei in Deutschland wegen »Zoombombing«, berichtet das Onlinemagazin Vice. Bundesdatenschützer Ulrich Kelber warnt vor dem Einsatz von Zoom und stellt abhörsichere Videochats ab dem Jahr 2022 in Aussicht.

30. Mai 2020: Das Nachrichtenportal MSN von Microsoft wird zukünftig von einer künstlichen Intelligenz (KI) bestückt und nicht mehr von Journalisten. 50 Angestellte und Redakteure, die bisher Redaktionspläne erstellt haben, Nachrichten und Geschichten für das Portal ausgewählt und produziert haben, verlieren ihren Job. Die Entscheidung, Menschen durch Maschinen zu ersetzen, ist nicht ohne Risiko: In Zukunft entscheidet eine Software darüber, welche Inhalte veröffentlicht werden, auch ob die Nutzer gewaltverherrlichende, pornografische oder sonst wie unangemessene Inhalte zu sehen bekommen. Dass die Software nicht fehlerlos arbeitet, konnte man jüngst an einem Bericht über die britische Popgruppe Little Mix sehen, der sich mit den Rassismus-Erfahrungen der Sängerin Jade Thirlwall beschäftigte. Illustriert wurde der Artikel mit einem Foto der ebenfalls nicht-weißen Bandkollegin Leigh-Anne Pinnock. Die englische Zeitung *Guardian* fragte, warum Microsoft eine offensichtlich rassistische Gesichtserkennungssoftware benutze, die gerade nicht-weiße Menschen nicht auseinanderhalten könne. Laut *Guardian* wurden die noch verbliebenen MSN-Redakteure angewiesen, sollte der Algorithmus kritische Berichte über ihren »Roboterjournalismus« (Spiegel) als interessant für den MSN-Leser identifizieren und automatisch auf die Seite stellen, sollten die Redakteure diese umgehend wieder von der Seite entfernen.

27. Mai 2020: Der Kurznachrichtendienst Twitter hat erstmals einen Tweet von US-Präsident Donald Trump mit einem Faktencheck belegt. Trump stellte die Behauptung auf, dass Briefwahl den Wahlbetrug fördere. Twitter versah den Präsidenten-Tweet mit dem Link »Erfahren Sie die Fakten über Briefwahl«, dort

wurde Trumps Behauptung als »unbegründet« zurückgewiesen. Trumps Reaktion an seine 88 Millionen Follower: Twitter unterdrücke das Recht auf freie Meinungsäußerung und wolle Einfluss nehmen auf die Präsidentschaftswahl. Auch Facebook-Chef Mark Zuckerberg kritisierte Twitters Faktencheck, soziale Netzwerke wie Facebook seien nicht der Schiedsrichter für die Wahrheit im Netz. Am Tag nach dem ersten kommentierten Präsidenten-Tweet kündigte Trump eine Verfügung gegen Social Media in den USA an.

22. Mai 2020: Ein Schweizer Software-Entwickler ist im Internet zufällig – via Google-Suchanfrage – auf sensible Daten von Mercedes-Benz-Fahrzeugen gestoßen. Der Quellcode für smarte Komponenten war gar nicht oder höchst unzureichend geschützt. Ohne Zugangsberechtigung konnte der Entwickler sich für das Git-Webportal von Daimler registrieren und anschließend auf mehr als 580 Git-Repositorys, inklusive Passwörter und API-Tokens, zugreifen und herunterladen. Unter anderem kam er so auf den Quellcode der in Mercedes-Transportern installierten Onboard Logic Units (OLU), die die Fahrzeuge mit der Cloud verbindet. Mit der OLU kann man die Standorte der Fahrzeuge online verfolgen oder, im Falle eines Diebstahls, stilllegen.

20. Mai 2020: Die Fluggesellschaft Easyjet wurde Opfer eines Hackerangriffs. Unbekannte Täter konnten Informationen zu rund neun Millionen Kunden abgreifen, darunter E-Mail-Adressen, Kontaktinformationen und Reisebuchungen, teilte die Airline mit. Bei über 2000 Kunden wurden auch Kreditkarten-informationen gekapert. Wie es zu dem Datenzugriff kommen konnte, konnte Easyjet nicht erklären.

18. Mai 2020: Bundesdatenschützer Ulrich Kelber hat die Behörden vor der Nutzung des Messenger-Dienstes WhatsApp gewarnt. Der zum Facebook-Konzern gehörende Dienst sei für eine Bundesbehörde ausgeschlossen, heißt es in einem Schreiben Kelbers an alle Ministerien. Behörden hätten bei der Einhaltung

des Datenschutzes, der gerade in Coronazeiten nicht vernachlässigt werden dürfe, eine Vorbildwirkung. Durch das Senden einer WhatsApp-Nachricht würden Metadaten erhoben, die, davon sei auszugehen, unmittelbar an Facebook weitergegeben würden, mit dem Ziel einer verstärkten Profilbildung der Nutzer. Mit dem hiesigen Datenschutzrecht sei das nicht vereinbar. WhatsApp widersprach Kelber, Metadaten würden nicht erhoben.

15. Mai 2020: Mehrere sogenannte Supercomputer wurden in Europa gleichzeitig von Unbekannten gehackt und wegen Sicherheitsproblemen vom Netz genommen. Darunter auch neun der leistungsfähigsten Rechenzentren in Deutschland, so das Leibniz Supercomputing Center in Garching bei München, das Stuttgarter Höchstleistungszentrum oder die beiden »Superhirne« des Karlsruher Instituts für Technologie. Über gekaperte Nutzerzugänge verschafften sich die Hacker Zugriff auf die Rechenzentren und konnten so ihre Nutzungsrechte bis zu »Root-Privilegien« ausweiten und damit nach Belieben schalten und walten. In der Folge konnten sie Zugangsdaten anderer Nutzer abfangen. Noch ist unklar, ob Forschungsdaten gestohlen werden konnten und wer dahintersteckt.

15. Mai 2020: Eine interne Dienstvorschrift namens »Signals Intelligence« belegt, wie der Bundesnachrichtendienst (BND) digital überwachen darf. So kann der BND an den 23 Internetknotenpunkten in Deutschland pro Tag bis zu 1,2 Billionen Verbindungen abzweigen – völlig legal. Als Auslandsnachrichtendienst darf der BND aber nur in Ausnahmefällen deutsche Staatsbürger überwachen, etwa wenn sie sich dem »Islamischen Staat« angeschlossen haben. Ob durch die nachrichtlichen Suchbegriffe, die sogenannten Selektoren, tatsächlich deutsche Staatsbürger von Ausländern strikt unterschieden werden können und wie groß der illegale »Beifang« ist, darüber streiten IT-Experten und Geheimdienstler.

13. Mai 2020: Der Hackerangriff auf den Deutschen Bundestag vor fünf Jahren ging vom russischen Geheimdienst aus, das

sei jetzt erwiesen, erklärte der Generalbundesanwalt. Nach jahrelangen Ermittlungen hat die Bundesanwaltschaft in der vergangenen Woche einen internationalen Haftbefehl gegen den jungen russischen Hacker Dimitri Badin erwirkt. Der Angriff hatte im Mai 2015 die IT-Infrastruktur des Bundestags komplett lahmgelegt, das deutsche Parlament musste tagelang vom Netz genommen werden. Die Angreifer waren mit E-Mails, die vorgaben, von den Vereinten Nationen zu sein, in die Systeme des Bundestags gelangt. Welche sensiblen Daten genau in russische Hände gelangten, ist unklar. Bundeskanzlerin Angela Merkel spricht von »hybrider Kriegsführung«.

13. Mai 2020: Die Technischen Werke Ludwigshafen (TWL) haben einen Hackerangriff und eine Erpressung von Cyberkriminellen öffentlich gemacht. Bereits Mitte Februar hätten Unbekannte 500 Gigabyte an Kunden-, Mitarbeiter- und Geschäftsdaten erbeutet, offensichtlich mit einem infizierten E-Mail-Anhang. Eine Verschlüsselung der Systeme sowie einen Zugriff auf die Prozessleittechnik konnte erfolgreich verhindert werden, die Versorgung der Stadt sei nicht gefährdet gewesen, teilte der kommunale Energie- und Wasserversorger mit. Trotzdem haben die Hacker einen zweistelligen Millionenbetrag gefordert, den die TWL abgelehnt habe. Die Täter hätten daraufhin die Daten im Darknet veröffentlicht und alle Kunden angeschrieben, um weiteren Druck auszuüben. Das LKA warnt davor, dass die erbeuteten Daten wie Adresse, Telefonnummern und Bankdaten zu weiteren Straftaten wie Identitätsdiebstahl genutzt werden können.

13. Mai 2020: Facebook hat bekannt gegeben, dass es mehr als 10.000 Content-Prüfern insgesamt 52 Millionen Dollar Entschädigung für die im Job erfahrenen psychischen Belastungen zahlen will. Hintergrund ist eine Sammelklage von ehemaligen US-Mitarbeitern vor dem Kammergericht im kalifornischen Bezirk San Mateo. Betroffene, die in Zusammenhang mit ihrer Tätigkeit bei Facebook erkrankten, können nun mit einer me-

dizinischen Behandlung sowie Schadenersatz von bis zu 50.000 Dollar rechnen. Externe Auftragnehmer hatten Facebook 2018 verklagt, weil das Social Network sich nicht angemessen um die Betreuung seiner sogenannten »Moderatoren« gekümmert hatte. Content-Prüfer müssen wiederholt drastische Inhalte wie Kindesmissbrauch, Enthauptungen, Terrorakte, Tierquälerei und andere verstörende Bilder und Videos sichten und filtern. Im Januar 2020 bezeichnete auch die Gewerkschaft Verdi die Arbeitsbedingungen der Facebook-Moderatoren in Deutschland als »prekär«, angesichts befristeter Arbeitsverträge, schlechter Bezahlung und der hohen Belastung.

21. April 2020: Der Chaos Computer Club (CCC) hält die Datenspende-App des Robert Koch-Instituts für »auf Dauer nicht tragbar«. Die App, die für Fitnesstracker und Smartwatches programmiert ist und die bereits 400.000 Nutzer hat, soll bei der Eindämmung der Covid-19-Pandemie helfen. Neuartige Algorithmen können in den Daten zu Aktivität, Herzfrequenz oder Postleitzahlen zusätzliche Informationen zur Verbreitung des Virus liefern, heißt es im Werbetext der App, die den Datenschutz nach eigener Aussage berücksichtige. CCC kritisiert hingegen die Schwachstellen der App, etwa, dass Fitnessdaten direkt vom Server des Anbieters oder von Google Fit an den RKI-Server übertragen werden. Dieser direkte Zugang erlaube Zugriff zu nicht pseudonymisierten Fitnessdaten bis hin zu den vollständigen Namen der Datenspender. Schlecht geschützt sei auch die Verknüpfung der App mit den Fitnesstrackern, die von Hackern ausgelesen werden könnte.

19. März 2020: Im Kampf gegen die Ausbreitung des Coronavirus hat das EU-Mitglied Litauen die Bewegungsprofile von Infizierten veröffentlicht. Auf einer Website hat der litauische Rundfunk eine Übersicht über alle bisher bekannten Fälle online gestellt. Die fortlaufend aktualisierten Daten stammen vom Nationalen Gesundheitszentrum. Angegeben wird, wann und an welchen Orten sich die Personen aufgehalten haben, ob sie pri-

vate oder öffentliche Verkehrsmittel benutzten, wann erstmals Symptome auftraten und wann sie diagnostiziert wurden. Litauen hat bisher 34 nachgewiesene Infektionsfälle. Die Deutsche Telekom hat dem Robert Koch-Institut anonymisierte Standortdaten von Millionen von Kunden zur Verfügung gestellt, um das Mobilitätsverhalten und die damit verbundene Ansteckungsrate in der Bevölkerung beobachten zu können. Die Nutzer wurden nicht einzeln darüber informiert, da keine personenbezogenen Daten herausgegeben wurden. Anfang April veröffentlichte Google auf der Basis seiner Millionen Android-Smartphones die Bewegungsdaten für 131 Länder. Es soll den Behörden ermöglichen, die Eindämmung des Virus und die Einschränkung der Bewegungsfreiheit der Menschen besser verstehen zu können. Google sagt, alle Daten wurden anonymisiert, überprüft werden konnte das nicht.

28. Februar 2020: Das Landeskriminalamt Niedersachsen warnt vor Fake Onlineshops, die im Zuge der Coronakrise im Internet angeblich Atemschutzmasken, Schutzkleidung oder Desinfektionsmittel verkaufen würden. So hätten Cyberkriminelle mit der Adresse PharmacyFirstGmbH.com den Namen eines realen deutschen Unternehmens missbraucht und mit Spammails mögliche Kunden angeschrieben. Das LKA warnt davor, Täter würden die Angst vieler Menschen vor dem Virus schamlos ausnutzen. Im März warnt das LKA Hessen vor gefälschten Formularen für die Corona-Soforthilfen des Staates, Hacker könnten Daten und Identitäten missbrauchen.

14. Februar 2020: Sicherheitsexperten vom Massachusetts Institute of Technology (MIT) haben nachgewiesen, dass die Wahl-App Voatz, die in den USA seit zwei Jahren zum Einsatz kommt, jeglicher Manipulation Tür und Tor öffnet. Hacker könnten, wenn sie es darauf anlegten, nicht nur mitlesen, für welchen Kandidaten ein Wähler auf seinem Smartphone gestimmt hat, die Täter könnten sogar die Wahlstimme fälschen oder ganz die Kontrolle über den Voatz-Server übernehmen und damit das