H 7625

FIfF Kommunikation

Zeitschrift für Informatik und Gesellschaft

38. Jahrgang 2021 Einzelpreis: 14 EUR 2+3/2021 – September 2021

Datenschutz

Usability

Barriere-freiheit

Informationssicherheit

ISSN 0938-3476

• Homeoffice und Gesundheit • Cyberpeace • BigBrotherAwards • Netzpolitik.org •

FIfF-Kommunikation

Zeitschrift für Informatik und Gesellschaft

Titelbild: Line art drawing of Pegasus. Archives of Pearson Scott Foresman, *https://commons.wikimedia.org/wiki/Category:Pegasus?uselang=de#/media/File:Pegasus_(PSF).png*

Inhalt

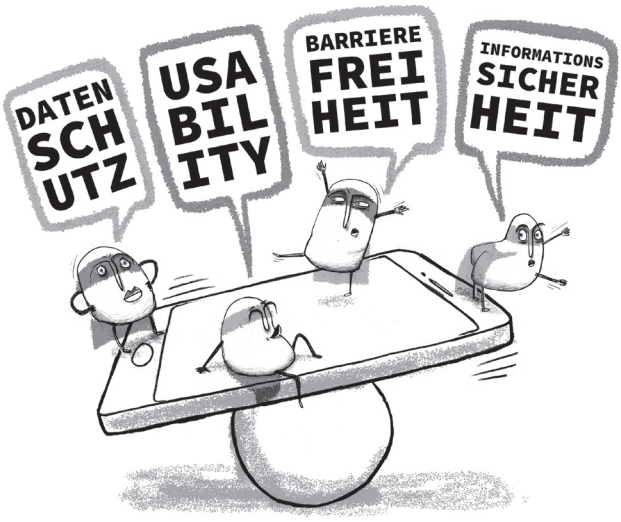
Ausgabe 2+3/2021

inhalt

Editorial

Auch in dieser Ausgabe der *FIfF-Kommunikation* widmen sich mehrere Beiträge den Themen der FIfF-Konferenz 2020 – *Vereinbarkeit und Widersprüche der Designziele Datenschutz, IT-Sicherheit, Usability und Barrierefreiheit*:

> *„Datenschutz, Informationssicherheit, Usability und Barrierefreiheit sind allgemein gesellschaftlich erwünschte Designziele und Anforderungen für Informationssysteme, die sich aber teilweise widersprechen. Wie können sie gemeinsam umgesetzt werden, wo stehen sie im Widerspruch? Wie können sie gesellschaftspolitisch realisiert und ausgehandelt werden?*



Dazu enthält die Ausgabe zwei Beiträge: Eine Einführung in *Usable Security und Privacy* gibt Stephan Wiefling. Er behandelt die Schutzziele von IT-Systemen und betrachtet sie vor dem Hintergrund der Usability. Sein Fazit: Es gibt keine Security ohne Usability; Sicherheit geht nur gemeinsam mit entsprechend befähigten Nutzerinnen und Nutzern.

Menschengerechte Sicherheit behandelt Zinaida Benenson in ihrem Beitrag. In zwei Studien, die sie mit ihrer Forschungsgruppe zu Phishing und Antivirus-Meldungen durchgeführt hat, haben sich Defizite gezeigt. Nutzerzentrierter Schutz erfordert nutzerzentriertes Denken: Wie sollen Angriffe gemeldet werden? Wie werden die Nutzer über Angriffe informiert? Was sollen sie im Angriffsfall tun und vor allem: Sind sie dazu in der Lage?

Neben diesem Schwerpunkt enthält die Ausgabe eine Reihe von aktuellen Beiträgen. Wir starten zunächst mit einer neuen Kolumne zu einem alten Thema: *Cyberpeace – für Frieden, Freiheit und eine lebenswerte Welt*. Hans-Jörg Kreowski und Aaron Lye betreuen die Kolumne, die ab sofort in jeder Ausgabe erscheinen soll. In diesem Heft befasst sie sich unter anderem mit dem jüngsten Skandal staatlicher Überwachung – *Pegasus* – und der Kampagne *Heimatland Erde*.

Impfungen sind ein wesentliches Mittel, die immer noch nicht ausgestandene Covid-19-Pandemie zu bekämpfen. Doch während man privilegierte Deutsche offenbar mit Bratwürsten locken muss, haben viele Menschen in großen Teilen der Welt überhaupt nicht die Möglichkeit einer Impfung. Gemeinsam mit anderen NGOs fordern wir die Bundesregierung und die EU-Kommission auf, die weltweite Bekämpfung der Pandemie nicht durch falsch verstandenen Schutz *geistigen Eigentums* zu blockieren.

Hans-Jörg Kreowski und Wolfgang Krieger zeichnen in ihrem Beitrag *Künstliche Intelligenz – ‚künstlich' ja, ‚Intelligenz' wohl kaum* deren Geschichte von den mit ebenso großen wie unrealistischen Erwartungen verbundenen Anfängen in den 50er-Jahren bis zum aktuellen Hype nach. „Es ist ... dringend geboten, das Mögliche und Wünschenswerte vom Märchenhaften, Phantastischen und Schrecken Einflößenden zu trennen und die weitere Entwicklung kritisch zu begleiten", stellen sie fest.

Das Arbeiten im Home-Office ist ein probates Mittel zur Eindämmung der Pandemie – zumindest wenn Tätigkeit und häusliches Umfeld dies erlauben. Anja Gerlmaier untersucht in ihrem Beitrag *Gesund arbeiten im Home-Office: Was lehrt uns die Corona-Krise,* ob das Home-Office ein erstrebenswertes Zukunftsmodell darstellt. Was müssen dabei die Betriebe tun? Sie stellt arbeitswissenschaftliche Erkenntnisse zum mobilen Arbeiten dar und gibt Gestaltungsempfehlungen.

Auch in diesem Jahr wurden in Bielefeld die *BigBrotherAwards* vergeben – wie in jedem Jahr berichten wir darüber. Neben einer Zusammenfassung der Gala dokumentieren wir zwei Laudationes: padeluun wendet sich gegen die unermüdlich vorgetragene Behauptung, Datenschutz würde eine effektive Bekämpfung der Covid-19-Pandemie verhindern und damit Menschenleben kosten. Rena Tangens thematisiert die immer weiter ausufernde Überwachung, die nicht zuletzt auf neueste psychologische Erkenntnisse setzt, um unsere Daten und unser Nutzer:innenverhalten effektiv und umfassend auszuspähen.

Um Überwachung geht es auch in der Rubrik *netzpolitik.org.* Es werden unter anderem erneut die Spähsoftware *Pegasus*, die nach heftigen Protesten 2019 nun doch erschreckend geräuschlos im Bundestag durchgewinkten *Upload-Filter* und die Defizite der Digitalisierung angesichts der Pandemie behandelt. Eine Filmkritik von Marit Hansen zum Film *Alles ist eins. Außer der 0* über Wau Holland und eine Reihe von Rezensionen und Ankündigungen aktueller Publikationen runden die Ausgabe ab.

Gestattet sei an dieser Stelle ein Hinweis in eigener Sache: Bekanntlich wird die *FIfF-Kommunikation* durch eine ehrenamtliche Redaktion betreut. Leider ist es aus unterschiedlichen Gründen nicht gelungen, die geplante Ausgabe 2/2021 rechtzeitig fertigzustellen. Wir haben uns deswegen entschieden, erstmals in der Geschichte der *FIfF-Kommunikation* zwei Ausgaben – 2/2021 und 3/2021 – zu einer Doppelausgabe zusammenzulegen. Klar, dass diese Lösung nicht befriedigt und wir sie künftig, wie auch schon bisher, möglichst vermeiden werden.

Gerade blicken wir fassungslos auf Afghanistan und die Ereignisse beim Abzug der internationalen Truppen. Momentan muss im Vordergrund stehen, Menschen in Sicherheit zu bringen, die durch die Machtübernahme der Taliban in Gefahr geraten sind – befremdlich, wenn sich manche anscheinend weniger Sorgen um Menschenleben machen als um Flüchtlinge, die nach

Deutschland kommen könnten. „2015 darf sich nicht wiederholen." – Ist das alles, was Euch dazu einfällt, liebe CDU? Warum so lange gezögert wurde, Menschen auszufliegen, und warum offenbar zusätzlich bürokratische Hürden aufgebaut wurden, wird hoffentlich noch untersucht werden. Doch die Ereignisse werfen auch erneut die grundsätzliche Frage nach solchen Einsätzen auf. Frieden, Demokratie und Menschenrechte lassen sich nicht militärisch erzwingen. Wenn man darauf abzielt, dass „… unsere Sicherheit auch am Hindukusch verteidigt wird" – so im Dezember 2002 der damalige Verteidigungsminister Peter Struck –, dann muss man mindestens wissen, was man eigentlich damit erreichen will und kann, was man genau verteidigen will – und wie. Das Thema wird sicherlich auch das FIfF und die *FIfF-Kommunikation* weiter beschäftigen.

Wir wünschen unseren Leserinnen und Lesern eine interessante und anregende Lektüre – und viele neue Erkenntnisse und Einsichten.

Stefan Hügel
für die Redaktion

Der Brief

Keine Experimente!

Liebe Freundinnen und Freunde, liebe Mitglieder des FIfF,

„Keine Experimente!" Das war 1957 der Wahlkampfslogan, mit dem Konrad Adenauer mit seiner CDU/CSU das höchste Ergebnis in deren Geschichte erzielte. Damals war mit „Experimenten" gesellschaftlicher Fortschritt gemeint, der heute längst selbstverständlich ist. Die damaligen Vorstellungen unserer Gesellschaft werden heute nur noch von Ultra-Konservativen und Rechtspopulisten geteilt – immer noch genügend, um CDU/CSU und AfD hohe Wahlergebnisse zu verschaffen.

Die Experimente, die heute mit unserer Gesellschaft angestellt werden, sind längst andere. Immer noch haben wir es mit den Folgen der Corona-Pandemie zu tun. Zeitweilig rückläufige Inzidenzwerte wiegten uns in trügerischer Sicherheit; inzwischen steigen die Werte wieder deutlich an. Offenbar ist es immer noch nicht begriffen worden, was exponentielle Prozesse bedeuten, wie schnell ein vermeintlich langsames Wachstum in schnelles Wachstum umschlagen kann und wie es sich dann immer stärker beschleunigt.[1]

Die vierte Welle, die durch die Delta-Variante des Corona-Virus verursacht wird, ist in einigen Ländern bereits voll ausgebrochen – beispielsweise in Großbritannien, wo auch eine Reihe von Spielen der Männer-Fußball-Europameisterschaft stattfand. Hier wurde bewusst in Kauf genommen, dass Fußballfans, die durch ganz Europa zum Spiel *ihrer* Mannschaft reisen, die Virusvariante in ganz Europa verbreiten – eine unfassbare Verantwortungslosigkeit.[2]

Der Wunsch vieler Menschen, nach der langen Zeit des Lockdown wieder zu verreisen und auch wieder richtig Urlaub machen zu können, ist verständlich. Damit Menschenleben zu gefährden, ist aber nicht akzeptabel.

Die Corona-Pandemie ist dennoch eine Krise, die wir voraussichtlich in absehbarer Zeit überwinden werden. Dabei spielt die Impfung der Bevölkerung eine entscheidende Rolle. Wir können auch künftige Pandemien nicht ausschließen, aber wir können dank des wissenschaftlichen Fortschritts darauf hoffen, ein Mittel dagegen zu finden.

Anders bei der *Klimakrise*, dem zweiten Experiment mit der Weltgesellschaft. Eine Krise ist irgendwann zu Ende. Beim Klimawandel handelt es sich aber um eine langfristige Entwicklung, die wir nur verlangsamen, im günstigsten Fall stoppen, aber nur langfristig wieder rückgängig machen können. Gerade beobachten wir die Hitze und die verheerenden Waldbrände im Westen von Kanada. Die Überflutungen in Rheinland-Pfalz und Nordrhein-Westfalen sind uns in frischer, beklemmender Erinnerung. Wir müssen uns wohl darauf einstellen, dass solche extremen Wetterereignisse und die damit verbundenen Opfer künftig zur traurigen Gewohnheit werden. Der kürzlich erschienene erste Teil des neuen Weltklimaberichts[3] stellt eine düstere Prognose – und sollte doch keine Überraschung sein.

Damit kommen wir zur Bundestagswahl. Robert Habeck, der Co-Vorsitzende der Grünen, hat darauf hingewiesen, dass Klimaschutz langfristiger Freiheitsschutz ist.[4] Wenn wir heute moderate Einschränkungen akzeptieren, tun wir dies, um unumgängliche und weit drastischere Freiheitseinschränkungen in der Zukunft zu vermeiden. Alle einschlägigen Statistiken der Klimaentwicklung zeigen deutlich: Je länger wir warten, desto weniger Zeit bleibt uns und desto drastischer müssen die Maßnahmen sein.

Nun ist es nichts Ungewöhnliches, dass gerade Politiker:innen, die tatsächlich oder vermeintlich einen Politikwechsel anstreben, in besonderer Weise angegriffen werden. Gerade habe ich Konrad Adenauer erwähnt: Die Angriffe auf Willy Brandt, in denen im Wahlkampf dessen uneheliche Geburt thematisiert wurde (ja, damals war das noch ein Thema), sind ein besonders schäbiges Beispiel.

Es kann also nicht überraschen, dass alle diejenigen, die das *Weiter so* auch beispielsweise beim Klimawandel zur Maxime ihrer Politik machen, eine grüne Bundeskanzlerin unter allen Umständen verhindern wollen. Da kommen aufgehübschte Lebensläufe[5], nicht rechtzeitig gemeldete Einkünfte[6] oder angebliche „Plagiate"[7] in einem der üblicherweise ohnehin eher belanglosen Bücher, die Politiker:innen halt schreiben, wenn sie ein Amt anstreben, gerade recht. Andere Parteien sind über derartige Vorwürfe selbstverständlich erhaben.[8] Die Grünen reagieren dünnhäutig. Doch sie machen es sich zu einfach, wenn sie in erster Linie Sexismus hinter solchen Angriffen wittern. Ohne-

hin dürfte der Druck im Wahlkampf nur ein lauer Vorgeschmack für den Druck sein, dem die Amtsinhaberin später ausgesetzt sein wird, wenn sie Entscheidungen treffen muss, von denen das Wohlergehen und manchmal auch das Leben vieler Menschen abhängen.

Wenn die üppig mit Geld der Wirtschaftslobby ausgestattete *Initiative neue soziale Marktwirtschaft* (INSM) Annalena Baerbock als „Moses" mit den „Zehn Verboten" darstellt, bedient das antisemitische Stereotype.[9] Nun ist der Vorwurf des Antisemitismus heute maximal diskreditierend – zu Recht. Da wollte sich CDU-Generalsekretär Ziemiak nicht lumpen lassen und trötete nach einem aus seiner Sicht antisemitischen Zitat von Carolin Emcke – die über diesen Verdacht nun wirklich erhaben ist – auf Twitter sofort los.[10] Nachdem er dann anscheinend mit Frau Emcke geredet hatte, ruderte er zurück.[11] Vielleicht hat es seine Einsicht auch befördert, dass gerade in der aktuellen Ausgabe des Regierungsblättchens *Schwarzrotgold* Frau Emcke ebenfalls prominent zu Wort kommt.[12] Ob solches Geschrei auf Twitter wirklich etwas bewirkt oder es doch eher ein Sturm im Wasserglas ist, sei dahingestellt. Nachdem es bei manchen Zeitungen inzwischen offenbar als Journalismus gilt, Twitter-Feeds abzuschreiben, erzielen solche Kleinodien der politischen Kommunikation durchaus ihre Wirkung.

Die aktuelle Form der politschen Debatte ist wohl kaum angemessen angesichts der wichtigen Weichenstellungen, die uns bevorstehen: Von der Bekämpfung des Klimawandels und den dafür angemessenen politschen, wirtschaftlichen und technischen Maßnahmen hängt nicht nur unser Fortbestand und der Fortbestand der Tier- und Pflanzenwelt ab. Auch wirtschaftlich werden wir künftig nur erfolgreich bleiben, wenn wir uns an den Erfordernissen des Klimas orientieren. Es ist ein verhängnisvoller Irrtum, dass wir regelmäßig „Wirtschaftskompetenz" mit einer Politik verwechseln, die die Bedürfnisse von Wirtschaftsunternehmen in den Vordergrund rückt. Die andauernde Covid-19-Krise bleibt eine große Herausforderung. Und wir dürfen die Übernahme außenpolitischer Verantwortung nicht länger mit militärischen Abenteuern verwechseln. Das 20-jährige Desaster in Afghanistan hat uns das gerade deutlich vor Augen geführt. Trotzdem werden Militäeinsätze als Mittel der Außen- und Sicherheitspolitik kaum mehr grundsätzlich hinterfragt. Und hier sind wir bei politischen Inhalten, die wir vor der Bundestagswahl vielleicht mal diskutieren sollten: Keine der Parteien, die sich um das Bundeskanzleramt bewerben, hat sich eindeutig gegen Killerdrohnen positioniert – bestenfalls gibt es wachsweiche Vorbehalte. Das geänderte Urheberrecht[13], mit den in Artikel 17 (vormals Artikel 13) geregelten Upload-Filtern, gegen das 2019 viele, vor allem junge Menschen auf die Straße gegangen waren, wurde im Bundestag ohne viel Aufhebens durchgewunken. Leider konnten sich auch die Grünen nur zu einer Enthaltung durchringen – vielleicht wollten sie sich ja keine Koalitionsoptionen verbauen.

Auch an der Überwachungsfront gibt es Neuigkeiten: Die Überwachungssoftware *Pegasus* wurde auf Smartphones von Journalist:innen, Menschenrechtler:innen, deren Familienangehörigen und Geschäftsleuten gefunden[14]. Eine Liste potenzieller Ziele enthält offenbar mehr als 50.000 Telefonnummern, darunter ein Dutzend Staats- und Regierungschef:innen und mehr als 180 Journalistinnen und Journalisten[15]. Apple – dessen Außenkommunikation bisher Privatsphärenfreundlichkeit und Sicherheit betonte – wird dafür kritisiert, zu wenig für die Abdichtung seiner Betriebssysteme – auch gegen Pegasus – zu tun[16]. Stattdessen werden – „*One more thing …* " – eigene Backdoors in den Betriebssystemen geöffnet; Apple begründet das damit, Kindesmissbrauch aufzudecken[17]. Dafür soll Künstliche Intelligenz eingesetzt werden. Backdoors und Techniken zur Inhaltserkennung können bekanntlich immer auch für ursprünglich nicht intendierte Zwecke und Inhalte genutzt werden, beispielsweise durch autoritäre Regimes, um missliebige politische Inhalte zu finden. Zunächst soll die Technik in den USA eingeführt werden; vor der Ausweitung auf andere Länder seien noch juristische Fragen zu klären[18]. Nach heftigen Protesten hat Apple nun erst einmal erklärt, vorläufig auf die Einführung verzichten zu wollen.

Die Bundestagswahl muss die Weichen richtig stellen: den Klimawandel verlangsamen oder stoppen die fortdauernde Pandemie angemessen bekämpfen, militärische Abenteuer beenden. Und wir brauchen eine bessere gesetzliche Absicherung gegen die ausufernde Überwachung. Eine konsequente und – vor allem – wirksame Umsetzung des einst vom Bundesverfassungsgericht proklamierten, aber offenbar gerade völlig vernachlässigten Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme[19].

Im besten Sinne: Gesellschaftlicher Fortschritt, keine gefährlichen Experimente!

Mit FIfFigen Grüßen
Stefan Hügel

Anmerkungen

1 *Eine allgemeinverständliche Einführung, was exponentielle Wachstumsprozesse bedeuten und wo sie auftreten, bietet Christian Stöcker (2020) Das Experiment sind wir, München: Blessing. Vereinfacht ausgedrückt: Wer exponentielle Wachstumsprozesse nicht versteht, versteht nicht, wie sich die Welt und die Gesellschaft heute entwickeln.*
2 *https://www.fr.de/sport/fussball/em-2021-england-gegen-deutschland-unverantwortliche-zuschauerpolitik-der-uefa-90832272.html*
3 *https://www.ipcc.ch/report/sixth-assessment-report-working-group-i/*
4 *Helene Bubrowski (2021) „Wer des Klima schützt, schützt die Freiheit", https://www.faz.net/aktuell/politik/inland/habeck-wer-das-klima-schuetzt-schuetzt-die-freiheit-17385954.html*
5 *https://www.tagesschau.de/faktenfinder/baerbock-lebenslauf-101.html*
6 *https://www.tagesschau.de/inland/baerbock-bundestag-nebeneinkuenfte-101.html*
7 *https://www.tagesschau.de/faktenfinder/plagiat-urheber-fakten-101.html*
8 *https://de.wikipedia.org/wiki/Liste_von_Korruptionsaffären_um_Politiker_in_der_Bundesrepublik_Deutschland*
9 *Klar, war keine Absicht: https://www.insm.de/insm/presse/pressemeldungen/erklaerung-der-initiative-neue-soziale-marktwirtschaft*
10 *Tweet gelöscht. Sicherungskopie unter https://twitter.com/syt_tkmk/status/1404887622279958538*
11 *https://twitter.com/PaulZiemiak/status/1404885987273195528*
12 *Die Menschen immer wieder überzeugen. Gespräch mit Carolin Emcke und Christoph Möllers, in: Schwarzrotgold. Das Magazin der Bundesregierung, 2/2021. An dieser Stelle vielleicht bemerkenswert, dass auffällig Werbung für dieses Regierungsblättchen auf einer Seite geschaltet wurde, auf der massiv gegen Annalena Baerbock gehetzt wird. Honi soit qui mal y pense.*

13 *vgl. Christoph Bruch (2020) #saveyourInternet gegen Zensur. Neues Urheberrecht der Europäischen Union gefährdet die Meinungsfreiheit, Grundrechte-Report 2020*

14 *https://www.heise.de/news/Spyware-Neue-Ueberwachungsvorwuerfe-gegen-israelischen-Software-Anbieter-NSO-6141286.html*

15 *https://www.zeit.de/politik/ausland/2021-07/spionage-software-pegasus-cyberwaffe-ueberwachung-menschenrechte-enthuellung*

16 *https://www.heise.de/news/Sicherheitsforscher-Apple-tut-nicht-genug-fuer-die-Sicherheit-seiner-Nutzer-6146740.html*

17 *https://www.spiegel.de/netzwelt/gadgets/apple-wird-iphones-nach-fotos-von-missbrauch-durchsuchen-a-3880c0a8-3daa-4d53-9340-4a938cc5e33b*

18 *https://www.spiegel.de/netzwelt/gadgets/durchsucht-apple-bald-alle-meine-iphone-fotos-a-1233c8d8-4935-4d34-8e37-688ddd8b1fc4*

19 *https://de.wikipedia.org/wiki/Grundrecht_auf_Gewährleistung_der_Vertraulichkeit_und_Integrität_informationstechnischer_Systeme*

Hans-Jörg Kreowski, Aaron Lye

Cyberpeace – für Frieden, Freiheit und eine lebenswerte Welt

Willkommen bei dieser neuen Rubrik, die ab jetzt regelmäßig in der FIfF-Kommunikation erscheinen soll, um von aktuellen Entwicklungen rund um das Thema Cyberpeace zu berichten.

Was Fachkreise schon lange vorher wussten, wurde durch die Enthüllungen von Edward Snowden im Jahre 2013 einer breiten Öffentlichkeit bekannt: Die Geheimdienste der Welt betreiben eine umfassende Überwachung aller elektronischen Kommunikationsmedien. Um darüber hinaus darauf aufmerksam zu machen, dass diese Medien und insbesondere das Internet von Anfang an und in wachsendem Maße für militärische Zwecke genutzt wurden und werden, hat das FIfF die Cyberpeace-Kampagne gestartet. Die Hauptforderungen sind: die Ächtung jeglicher Form von Cyberkrieg und ein demokratisch gestaltetes und demokratisch kontrolliertes Internet, das dem Frieden dient, nicht der Ausspähung und Kriegsführung. Nähere Informationen findet man auf der Kampagnen-Webseite *https://cyberpeace.fiff.de/Kampagne/Home/*.

Im Zuge der Kampagne sind Tausende Aufkleber mit der Cyberpeace-Taube verteilt, viele Vorträge gehalten, viele Publikationen entstanden und viele Veranstaltungen durchgeführt worden, von zweistündigen Cyberpeace-Cafés bis zu zweitägigen Cyberpeace-Foren. Sehenswert ist der Kurzfilm *Cyberpeace statt Cyberwar!* von Alexander Lehmann, der mit Hilfe der bridge-Stiftung finanziert werden konnte. Und die Cyberpeace-Taube ist inzwischen zum FIfF-Logo geworden. Die Cyberpeace-Kampagne ist eine Erfolgsgeschichte.

Auf der FIfF-Klausurtagung Ende März diesen Jahres haben die Teilnehmenden verabredet, der Kampagne neuen Schwung und noch mehr Sichtbarkeit zu verleihen. Als ein wesentliches Element ist dabei an eine thematische Ausweitung gedacht: über Cyberpeace als Gegenkonzept zu Cyberkrieg hinaus. In gewisser Weise kann man Cyberpeace auch als Synonym für FIfF verstehen, denn „Cyber" deckt alles ab, was mit Informatik und Information- und Kommunikationstechnik zu tun hat, und „Peace" steht ja ohnehin für Frieden, womit nicht nur Abwesenheit von Krieg gemeint ist, sondern auch Abwesenheit von Unterdrückung und prekären Lebensverhältnissen. Die Cyberpeace-Kampagne richtet sich dementsprechend gegen alle Militär- und Waffensysteme, die auf Informations- und Kommunikationstechnologie basieren, gegen die Einschränkung von Grund- und Menschenrechten durch Überwachungssysteme und gegen die Zerstörung von Natur und Umwelt, an der auch der Einsatz von Technik einen gehörigen Anteil hat. Positiv ausgedrückt: geht es darum, wie die Methoden und Technologien der Informatik genutzt werden können, um friedliche, freiheitliche und faire Lebensbedingungen für alle Menschen auf der Grundlage eines nachhaltigen Wirtschaftssystems zu schaffen – eine lebenswerte Welt.

Die neue Rubrik ist gedacht für Ankündigungen, Berichte, kurze Texte und Stellungnahmen rund um das Thema Cyberpeace. Alle Leser:innen sind aufgerufen, die Rubrik für eigene Beiträge zu nutzen. Sie können jederzeit an uns geschickt werden: kreo@fiff.de und lye@fiff.de.

In dieser ersten Ausgabe folgen drei Mitteilungen: (1) KI zieht in den Krieg, (2) Eurodrohne und FCAS, (3) Kampagne Heimatland Erde sowie (4) The Pegasus Project.

(1) Künstliche Intelligenz zieht in den Krieg – Aufruf zur Einreichung von Beiträgen

In ihrer KI-Strategie von 2018 verkündet die Bundesregierung, dass sie Künstliche Intelligenz umfassend fördern will, damit in nahezu allen Bereichen von Staat und Wirtschaft durch KI-Anwendungen große Fortschritte erzielt werden können. Mehrfach wird betont, dass die Nutzung von KI verantwortungsvoll und am Gemeinwohl orientiert erfolgen soll. Anwendungen im militärischen Bereich werden nur am Rande vermischt mit Fragen der inneren Sicherheit erwähnt. KI-basierte Waffentechnik kommt überhaupt nicht vor. Tatsächlich aber wird in Politik, Militär und Wissenschaft weltweit die Entwicklung und die Anwendung von KI-Methoden und KI-Technologien für militärische Zwecke einschließlich Waffensysteme vorangetrieben: KI zieht in den Krieg.

Unter dieser Überschrift soll in zwei geplanten FIfF-Publikationen die Rolle von Künstlicher Intelligenz im militärischen Bereich vorgestellt, diskutiert und hinterfragt werden:

- Ein 16-seitiges Dossier mit sechs bis acht Beiträgen, das dem Heft 4/2021 von Wissenschaft und Frieden beigelegt werden soll.
- Ein 30- bis 40-seitiger Schwerpunkt in der FIfF-Kommunikation 4/2021 mit zehn bis zwölf Beiträgen.

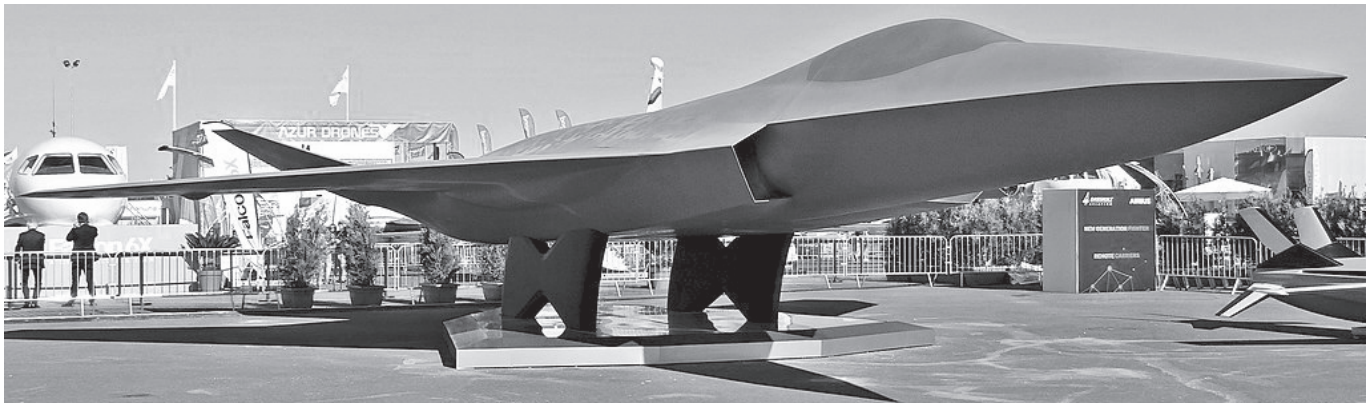
Die Sammlung von Beiträgen für das Dossier ist bereits abgeschlossen. Die Beiträge für den Schwerpunkt mit 15.000 bis 20.000 Zeichen müssen bis Ende Oktober 2021 vorliegen.

Diese Ausschreibung wurde bereits Anfang Mai mit Einreichungsschluss 25. Mai 2021 über Mailinglisten verteilt. Angebote von Kurzentschlossenen können aber immer noch an *kreo@fiff.de* und *lye@fiff.de* geschickt werden, je bitte mit Angabe der Autor:innen, einem Titel und einer kurzen Inhaltsangabe von fünf bis zehn Zeilen. Wir werden versuchen, solche Angebote noch im Schwerpunkt unterzubringen.

(2) Eurodrohne und FCAS

Die Bewaffnung der geleasten Bundeswehr-Drohnen vom Typ Heron TP ist im Dezember 2020 am Veto der SPD-Fraktion vorläufig gescheitert. Ein kleiner Sieg der Vernunft. Das heißt aber noch lange nicht, dass es auch zukünftig dabei bleibt. Mehr noch steht die Frage der Bewaffnung dann bald auch für die Eurodrohne an. Ihre Entwicklung läuft seit einiger Zeit unter Leitung von Airbus als europäisches Projekt mit Deutschland, Frankreich, Italien und Spanien. Auch der Kauf von 21 Eurodrohnen für die Bundeswehr ist bereits beschlossene Sache. Das Projekt wird den deutschen Steuerzahler:innen viele Hunderte Millionen Euro kosten. Die Eurodrohne ist als Aufklärungsdrohne konzipiert, die auch bewaffnet werden kann. Mit der Auslieferung der ersten Exemplare an die Bundeswehr wird zum Ende dieses Jahrzehnts gerechnet. Europa soll mit der Eurodrohne unabhängig von nichteuropäischen Systemen werden und so auch militärisch souveräner. Durch europäische Zusammenarbeit sollen auch Kosten gespart werden, die durch den Verzicht auf solche Drohnen gar nicht erst entstünden. Die Bundeswehr wünscht sich bewaffnete Drohnen. CDU und CSU sind auch schon lange dafür. Die SPD macht erklärtermaßen ihre zukünftige Haltung davon abhängig, wie ein umfassender gesellschaftlicher Diskurs zum Für und Wider der Drohnenbewaffnung ausgeht. Eigentlich ist aber längst klar, dass sehr viel gegen solche Waffensysteme spricht. Dabei spielt es keine Rolle, ob sie bewaffnet oder unbewaffnet sind. Denn wenn eine Aufklärungsdrohne ein anzugreifendes Ziel „aufklärt" und andere Waffensysteme es zerstören, ist der Unterschied zu einer Drohne, die selbst schießt, marginal. Sie sind alle Killerdrohnen, die bisher tausendfach völkerrechtswidrig für gezielte Tötungen und mit Tausenden ziviler Opfer eingesetzt wurden. Auch der Einsatz türkischer Killerdrohnen durch Aserbaidschan im Krieg gegen Armenien im Herbst letzten Jahres war völkerrechtswidrig, weil Aserbaidschan angegriffen hat. Die Führung der Bundeswehr behauptet, dass sie Killerdrohnen nie völkerrechtswidrig einsetzen will. Das Gegenteil wäre ja auch hochgradig merkwürdig. Die Bundeswehr bleibt allerdings eine klare und überzeugende Antwort schuldig, wie sie diese Waffen stattdessen einsetzen will.

Noch wahnwitziger ist ein zweites europäisches Rüstungsprojekt, an dem sich vorläufig Deutschland, Frankreich und Spanien beteiligen und das gerade auf den Weg gebracht wird: das *Future Combat Air System* (FCAS). Im Zentrum steht die Entwicklung eines neuen Kampfflugzeugs, das ab 2040 die dann völlig veralteten Eurofighter und Rafale ablösen soll. Das Projekt umfasst aber weit mehr. Es soll ein System von Systemen werden, bei dem Kampfjets zusammen mit Lenkflugkörper- und Drohnenschwärmen in einer Weise eingesetzt werden sollen, die Europa in allen Teilen der Welt die Überlegenheit im Luftkampf sichert. Was sind das für Kriege, die Europa in der zweiten Hälfte des Jahrhunderts führen möchte und gegen welche Kriegsgegner? Aber nicht nur alle friedliebenden Menschen muss dieses gigantomanische Projekt, dessen Kosten im dreistelligen Milliardenbereich liegen wird, zutiefst erschrecken, sondern alle Informatiker:innen haben einen besonderen, fachbezogenen Grund, schockiert zu sein. Als methodisches und technologisches Kernstück von FCAS ist die Künstliche Intelligenz auserkoren. Es ist bisher noch ziemlich unklar, woran dabei im Einzelnen



Model of the Future Air Combat System (FCAS) at the Paris-Le Bourget 2019 Airshow

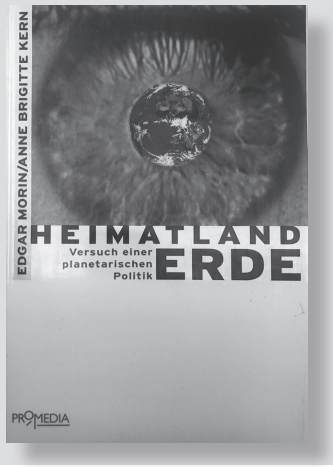
gedacht ist. Aber umso wichtiger ist, die Entwicklung mit großer Aufmerksamkeit zu verfolgen und einen wirkungsvollen Widerstand aufzubauen. FCAS muss verhindert werden.

Eine ausführliche Darstellung von FCAS findet man im Informationsbericht des französischen Senats: *http://www.senat.fr/rap/r19-642-3/r19-642-31.pdf*.

Eine erste kritische Analyse von Jürgen Wagner ist unter dem Titel *Future Combat Air System – Das größte Rüstungsprojekt Europas* als IMI-Studie 2021/4 erschienen: *https://www.imi-online.de/2021/07/13/future-combat-air-system-2/*.

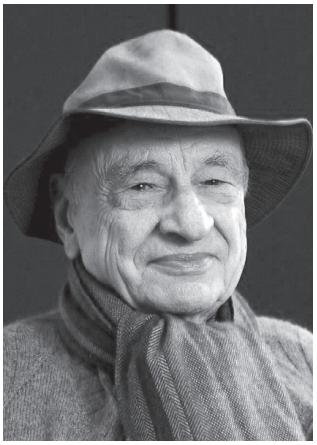
(3) Kampagne *Heimatland Erde*

Das Österreichische Studienzentrum für Frieden und Konfliktforschung (ASPR) hat die Kampagne *Heimatland Erde* zur Förderung des planetaren Bewusstseins gestartet. Das FIfF ist eine von über 50 Kampagnen-Partnerorganisationen aus aller Welt und dort in guter Gesellschaft.



Edgar Morin
Heimatland Erde.
Versuch einer planetarischen Politik
Promedia 1999
240 Seiten
Preis € 17,90 (brosch.)
ISBN: 978-3-85371-139-2

Die Menschheit steht neben der Eindämmung der Covid-19-Pandemie vor vielen weiteren globalen Herausforderungen. Hunger und Armut in der Welt sind gewachsen. Die Zahl der Flüchtlinge ist größer geworden, wobei die meisten von ihnen unter elenden Bedingungen und ohne jede Perspektive in Flüchtlingslagern hausen. Dagegen sind viele Reiche in schamloser Weise noch reicher geworden. Auch die Zahl der Kriege hat zugenommen. Die Bemühungen, den einen oder anderen Krieg zu beenden, sind kläglich. Echte Friedensverhandlungen, die zu einem fairen Interessenausgleich der verfeindeten Parteien und so zu dauerhaftem Frieden führen könnten, stehen nirgendwo auf der Tagesordnung. Die nationalen und internationalen Bemühungen, den menschengemachten Klimawandel und die Zerstörung von Natur und Umwelt zu stoppen, sind weit hinter den Erfordernissen zurückgeblieben. Die Menschheit ist dabei, sich ihrer Lebensgrundlagen zu berauben. Unterdrückung, Ausbeutung, Machtmissbrauch, Menschenrechtsverletzungen, Hass und Gewalt sind in vielen Teilen der Welt Alltag. Keines dieser Probleme lässt sich durch nationale Alleingänge lösen. Das geht nur durch gemeinsames weltweites Handeln auf globaler Ebene beim Überwinden der Ursachen. Das ist mit Heimatland Erde gemeint. Ziel der Kampagne ist, das Bewusstsein zu stärken, dass alle Menschen die Erde als Lebensraum teilen, dass es keine Alternative dazu gibt und dass die Menschheit nur überleben kann, wenn sie ihren Lebensraum nicht zerstört.



Edgar Morin 2011
Fronteiras do Pensamento, CC BY-SA 2.0

Mit der Kampagne wird der französische Philosoph Edgar Morin geehrt, der am 8. Juli 2021 seinen 100. Geburtstag feiert, in seinem 1993 erschienenen Buch *Terre Patrie*, das 1999 unter dem Titel *Heimatland Erde – Versuch einer planetarischen Politik* in deutscher Übersetzung publiziert wurde, hat er das Konzept entwickelt, das der Kampagne zugrundeliegt. Mehr Informationen findet man auf der Kampagnen-Webseite unter *https://www.heimatlanderde.com/* mit dem Kampagnenaufruf, dem Kampagnenmanifest, einem Videoaufruf von Edgar Morin und einer kurze Biographie des Philosophen. Auf der Webseite werden auch Mitmachmöglichkeiten aufgezählt. So kann man den Aufruf unterzeichnen, mithelfen, die Kampagne bekanntzumachen, oder sich an der Bastelaktion von Passhüllen für Erdenbürger:innen beteiligen. Insbesondere lud das Studienzentrum ASPR auch zu seiner 37. Sommerakademie zum Thema *Heimatland Erde – Friedenspolitik im Zeitalter des Anthropozäns* ein, die vom 1. bis 5. September 2021 online stattfand.

(4) The Pegasus Project: Ein Kommentar

Pegasus ist eine Schadsoftware/Malware, die vor allem iPhones und Android-Geräte infiziert. Sie ermöglicht es den Betreiber:innen des Tools, Daten wie beispielsweise Nachrichten in diversen Messengern, nachdem sie entschlüsselt wurden, aufgerufene Websites, Fotos und E-Mails oder auch Standort-Metadaten von dem Gerät zu extrahieren. Pegasus vermag Anrufe aufzuzeichnen, heimlich Mikrofon und/oder Kamera zu aktivieren oder auch beliebige Daten nachzuladen. Produziert wird die Software von der israelischen Firma NSO Group. Sie gehört zu den führenden Herstellern kommerzieller Spionagesoftware. Das Unternehmen verkauft weltweit Produkte an Militär, Strafverfolgungsbehörden und Geheimdienste und hat ca. 60 Kunden in 40 ungenannten Ländern.

Viele der Kunden nehmen Journalist:innen, Menschenrechtsverteidiger:innen, politische Gegner, Geschäftsleute und Staatsoberhäupter als Ziele dieser Software. Seit einigen Jahren ist die Software in der Presse. Kürzlich war das erneut der Fall. Mindestens 180 Journalist:innen in 20 Ländern wurden gezielt mit dieser Schadsoftware von mindestens 10 NSO-Kunden angegriffen. Dies geht einer Mitte Juli veröffentlichten Recherche des Pegasus-Projekts hervor, eines globalen Konsortiums von mehr als 80 Journalist:innen aus 17 Medien in zehn Ländern, die von Forbidden Stories mit technischer Unterstützung des Security Lab von Amnesty International koordiniert wurde.

Forbidden Stories und Amnesty International hatten Zugang zu mehr als 50.000 Datensätzen von Telefonnummern, die von NSO-Kunden zur Überwachung ausgewählt wurden. Die Telefonnummern, die möglicherweise im Vorfeld eines Überwachungsangriffs ausgewählt wurden, verteilten sich auf mehr als 45 Länder auf vier Kontinenten. Die Analyse der durchgesickerten Daten durch das Konsortium ergab, dass es sich bei mindestens zehn Regierungen um NSO-Kunden handelt, die Nummern in ein System eingegeben haben: Aserbaidschan, Bahrain, Indien, Kasachstan, Mexiko, Marokko, Ruanda, Saudi-Arabien, Ungarn und die Vereinigten Arabischen Emirate. Aus der Analyse der Daten geht hervor, dass Mexiko die meisten Nummern ausgewählt hat (mehr als 15.000). Von Mexiko ist seit 2017 bekannt, dass verschiedene Regierungsbehörden Pegasus gekauft und gegen Journalist:innen eingesetzt haben. Die Analyse der Daten zeigt, dass sowohl Marokko als auch die Vereinigten Arabischen Emirate mehr als 10.000 Nummern auswählten und mehr als 1.000 Nummern in europäischen Ländern ebenfalls von NSO-Kunden ausgewählt wurden. Neu ist nicht, dass die oben genannten Gruppen systematisch beobachtet werden. Aber es ist zweifelsohne wichtig, die Dimension und Techniken aufzuzeigen.

Eva Galperin, die Leiterin für Computersicherheit bei der Electronic Frontier Foundation (EFF), war eine der ersten Sicherheitsforscher:innen, die Anfang der 2010er Jahre Angriffe auf Journalist:innen und Menschenrechtsverteidiger:innen in Mexiko, Vietnam und anderswo identifizierte und dokumentierte. Seit diesen Anfängen ist die Installation von Spyware auf Smartphones subtiler geworden. Anstatt dass die Zielperson auf einen Link klicken muss, um die Spyware ungewollt zu installieren, ermöglichen sogenannte Zero-Click-Exploits, die Kontrolle über das Telefon zu übernehmen, ohne dass die Zielperson etwas tun muss. Dazu reicht es, die Telefonnummer zu kennen, um über das Netz anzugreifen. Ein physischer Zugriff vor Ort ist nicht nötig. Dass NSO bei Pegasus Zero-Click-Exploits einsetzt, ist seit spätestens 2015 bekannt. Die WikiLeaks Publikation Spy-Files belegt dieses mit geleakten internen E-Mails.

Bemerkenswert an der aktuellen Recherche ist neben der großen Anzahl auch, dass selbst (relativ) aktuelle iOS- und Android-Versionen betroffen sind. Folglich sind selbst Menschen, die sich der Problematik bewusst sind und Sicherheitsupdates einspielen, trotzdem angreifbar.

Die Konsequenz darf allerdings nicht Resignation sein. Vielmehr müssen wir uns erneut die Frage stellen, wie wir dem Problem individuell, als Informatiker:innen und als Gesellschaft begegnen.

Apple und Google haben kein Interesse daran, sichere Betriebssysteme zu entwickeln. Selbstverständlich haben sie Abteilungen, die sich mit den Angriffen und Gegenmaßnahmen beschäftigen. Allerdings ist der Druck von Regierungen, die immer wieder Hintertüren fordern, groß und es besteht bei den Konzernen ein großes Interesse, daran zu kooperieren.

Außerdem sind die Anreize, Exploits (auf dem Schwarzmarkt) zu verkaufen, größer als sie Software-Produzenten zu melden, damit die Sicherheitslücken geschlossen werden können. Dieses Geschäftsmodell als solches wird von Staaten befürwortet, da diese ja selbst Exploits kaufen (lassen) um Systeme anzugreifen.

Das Framing der Rechercheergebnisse, dass die Überwachungssoftware der israelischen Firma, die vermeintlich ja sonst nur für staatstragende Zwecke von Strafverfolgungsbehörden, Geheimdiensten und Militärs genutzt wird, jetzt von autoritären Staaten zweckentfremdet wird, ist ein Zerrbild der Realität und erweckt den Eindruck, dass es sich nicht um unser Problem handelt.

Auch deutsche Behörden sind Kunden der Überwachungsindustrie. Seit 2007 ist der Einsatz von kommerzieller Spionagesoftware bei Strafverfolgungsbehörden bekannt. Das bekannteste Beispiel ist das Produkt FinSpy von FinFisher, welches seit 2013 vom BKA eingekauft wird. Ständig werden die Befugnisse von Polizei und Geheimdiensten hierzulande ausgeweitet. Erst kürzlich hat eine Gesetzesverschärfung den Trojanereinsatz für allen 19 Geheimdienste legalisiert.

Wir alle wissen, dass Journalist:innen Informationen bekommen, an denen Geheimdienste ebenfalls interessiert sind und auch, woher diese stammen. Insbesondere, wenn es sich um undichte Stellen in der Regierung oder in einem für die Regierung wichtigen Unternehmen handelt. Wir wissen aus der Vergangenheit, dass Überwachung von Journalist:innen auch in der Bundesrepublik kein Tabu ist.

Die Weltöffentlichkeit kennt spätestens seit den Snowden-Enthüllungen das Ausmaß staatlicher Überwachung insbesondere der FiveEyes, aber auch anderswo. Die Repression gegen WikiLeaks und Assange zeigen die Konsequenz von nonkonformem Journalismus auf. Vielerorts werden Journalist:innen verschleppt und umgebracht. Das Bekanntwerden der Dimension der systematischen Überwachung von Journalist:innen ist ein harter Schlag für kritische Journalist:innen weltweit und schafft ein toxisches Klima bezüglich der Sicherheit und Vertraulichkeit von Quellen.

FIfF e. V. – Pressemitteilung

Wir fordern Bundesregierung und EU-Kommission auf, nicht weiter die weltweite Bekämpfung der Corona-Pandemie zu blockieren

Mit detaillierter FAQ

14. Mai 2021 – *Durch die Blockadehaltung von Bundesregierung und EU-Kommission wird der* TRIPS-Waiver *gefährdet. Die darin geforderte temporäre Freigabe der Corona-Impfstoffpatente ist ein essentieller Schritt für eine effektive globale und langfristige Bekämpfung der Pandemie. Es ist höchste Zeit, dass alle Regierungen der EU die Zeichen der Zeit erkennen und sich für den Antrag aussprechen.*

Wie in der FIfF-Pressemitteilung vom 24. April 2021[1] beschrieben, haben Südafrika und Indien im Oktober 2020 einen bemerkenswerten Vorstoß unternommen: Ihr Antrag fordert bei der WTO die vorübergehende Aussetzung der internationalen Verfolgung von Verstößen gegen geistige Eigentumsrechte auf Covid-19-Impfstoffe und anderer für die Pandemiebekämpfung nötiger medizinischer Technologien[2].

Im globalen Weltgefüge hat sich daraufhin eine deutliche Kluft aufgetan: Nahezu alle Länder des Globalen Südens haben sich dem Antrag angeschlossen oder unterstützen ihn, während sich die Länder des Globalen Nordens größtenteils dagegen aussprachen. Eine breite Front von Hilfsorganisationen unterstützt den TRIPS-Waiver und konnte in den letzten Tagen einen großen Erfolg vermelden: Katherine Tai – Handelsbeauftragte der USA – hat sich für den Waiver ausgesprochen. Dies ist eine Entwicklung, die noch vor kurzer Zeit als undenkbar galt. **Die politische Debatte um die Aussetzung der Patente hat dadurch auch in Europa neuen Schwung bekommen, wird jedoch unter anderem durch die deutsche Regierung blockiert.** Um den Weg für eine effektive globale Pandemiebekämpfung freizumachen, stellt das FIfF daher drei zentrale Forderungen:

1. **Wir fordern die Bundesregierung auf, den TRIPS-Waiver zu unterstützen. Die Aussetzung der Impfstoffpatente ist ein notwendiger Schritt hin zur Mobilisierung aller global verfügbaren Impfstoffproduktionskapazitäten. So wird Rechtssicherheit gewährt und der Ausbau der Produktion im globalen Süden grundsätzlich erlaubt.**

2. **Wir fordern die Bundesregierung auf, öffentlich geförderte Pharmaunternehmen in geeigneter Art zu verpflichten, sich am COVID-19 Technology Access Pool (C-TAP) oder vergleichbaren Programmen zu beteiligen und Technologietransfers in den globalen Süden zu unterstützen. So können die Länder des globalen Südens vollen Nutzen aus den neuen rechtlichen Rahmenbedingungen ziehen.**

3. **Wir fordern die Bundesregierung auf, auch über die Pandemie hinaus Regelungen zu schaffen, die sicherstellen, dass öffentlich geförderte medizinische Forschung direkt der Allgemeinheit zugutekommt und nicht künstlich verknappt wird, um Profitinteressen zu genügen (Öffentliches Geld – Öffentliches Gut).**

Moderne Pharma- und Biotechnologie ist ohne Informationstechnik undenkbar. An jedem Impfstoffrezept und in jedem Pharmaunternehmen arbeiten Naturwissenschaftler:innen, Ingenieur:innen und Informatiker:innen. Ohne deren Arbeit kann es die neuartigen Impfstoffe nicht geben. Sie ermöglichen, dass Covid-19 die erste Pandemie einer Atemwegserkrankung in der Geschichte werden kann, die weit hinter ihrem vollen zerstörerischen Potential zurückbleibt.

Es ist daher wichtig, dass auch wir als Informatiker:innen Stellung beziehen. Als Informatiker:innen wissen wir aus vielen anderen politischen Debatten, dass Gesetze zum geistigen Eigentum oft im Interesse Weniger und gegen die Interessen Vieler angewendet werden. Die Erschließung aller global zur Verfügung stehenden Impfstoffproduktionsmittel ist aber vor dem Hintergrund der Pandemie unerlässlich. Dies ist eine der größten sozialen Fragen der Gegenwart. Eine faire Verteilung ist nur möglich, wenn Impfstoffe nicht weiter künstlich verknappt werden.

Oft gestellte Fragen / FAQ[3]

Auch die FIfF-Pressemitteilung vom 24. April 2021[4] hat dazu beigetragen, die Diskussion in der Zivilgesellschaft anzuschieben. Uns haben in der Folge viele Zuschriften erreicht. Wir wollen hier auf einige Punkte genauer eingehen und damit Rüstzeug für die Meinungsfindung geben. An dieser Stelle sei auch noch einmal die sehr gute FAQ von Ärzte ohne Grenzen[5] empfohlen.

Frage: Für die Bekämpfung der Pandemie bewerben die wirtschaftlich starken Länder die Initiative COVAX. Was haltet ihr von dieser Alternative?

Antwort: COVAX ist völlig unzureichend und setzt die Abhängigkeit der Länder des Globalen Südens vom Globalen Norden fort. Die COVAX-Initiative zielt lediglich auf eine Versorgung von 20 Prozent der jeweiligen Bevölkerungen der beteiligten Länder bis Ende 2021 ab. Zudem werden selbst diese wenigen Dosen bisher nicht plangemäß bereitgestellt[6].Die WHO zeichnet ein bestürzendes Bild der bisherigen Impfstoffverteilung: Stand Anfang April 2021 wurden nur **0,2 % der 700 Millionen global produzierten Dosen in Länder mit niedrigen Einkommen verimpft**[7]. Solange die Abhängigkeit von Finanzierung und Spenden aus den Ländern mit hohem Einkommen fortbesteht, werden auch in Zukunft nur die „Überschüsse" weitergereicht werden.

Zudem benötigen wir schnellstmöglich Impfstoff, etwa viermal so viel, wie weltweit gerade jährlich produziert wird. Im Sinne einer schnellen und effektiven Bekämpfung der globalen Pandemie und getreu dem Grundsatz „Öffentliches Geld – öffentliches Gut" müssen Produktionskapazitäten dafür auf der ganzen Welt aufgebaut werden.

Frage: Wie genau würde die Aussetzung von Patenten von ärmeren Ländern genutzt werden können? Welche der ärmeren Länder sind denn in der Lage, eigene Fabriken aufzubauen und zu betreiben?

Antwort: Um Produktionskapazität aufzubauen, müssen die Länder es erstens *dürfen* und zweitens *können*. Das Dürfen wird durch den TRIPS-Waiver abgedeckt, das Können ist entweder bereits vorhanden oder muss durch Schulungen gewährleistet werden – klassischer Technologietransfer.

Die Fabriken müssen nicht erst gebaut werden. Die Vorstellung ist überholt, nur die westliche Welt hätte die technische Expertise, diese Produkte herzustellen. Diverse Länder des globalen Südens sind nachweislich in der Lage und bereit, in die Produktion dieser Güter einzusteigen bzw. diese Produktion auszuweiten. Das gilt zum Beispiel für Indien, Bangladesch, Uganda, Kuba, Argentinien, Brasilien und Pakistan[8]. Doch eine Aussetzung der Patentrechte würde eben auch ermöglichen, dass neue Produktionsstätten erschlossen werden können. Dass das innerhalb von wenigen Monaten geht, wurde in den letzten Monaten bewiesen.

So zeigt etwa jenes in der FIfF-Pressemitteilung vom 24. April 2021[9] beschriebene Beispiel der HIV/AIDS-Pandemie, dass der wichtigste Faktor für den Zugang zu Medikamenten im globalen Süden der Preis ist. Patente und andere Formen des geistigen Eigentums stehen aber der lokalen Produktion von günstigen Generika im Wege. Auch Nicole Lurie von der Coalition for Epidemic Preparedness Initiatives (CEPI) bestätigt: „*There is excess [vaccine production] capacity out there, still. The challenge is that right now the companies that have got established vaccines are really hesitant to form partnerships, particularly with some developing country manufacturers*."[10]

Damit z. B. interessierte Generika-Produzenten mit der Impfstoffproduktion beginnen können, brauchen sie auch die Rezepte für die Herstellung. Es gibt dafür bereits einige Initiativen, z. B. den COVID-19 Technology Access Pool (C-TAP)[11] und den COVID-19 mRNA vaccine technology transfer hub[12]. Der C-TAP wurde bereits im Mai 2020 von der WHO auf Initiative Costa Ricas gestartet. Er hat sich fünf Ziele gesetzt, die für eine schnelle Produktentwicklung und Versorgung wichtig sind:

1. Gensequenzen und Daten öffentlich verfügbar zu machen, um die Forschung zu beschleunigen;

2. Transparenz bei den Studienergebnissen herzustellen, damit es Klarheit über die besten Produkte gibt;

3. Regierungen und andere Geldgeber sollen ihre Zahlungen an Firmen und Forscher:innen an Bedingungen knüpfen: gerechter Zugang, günstige Preise und eine vollständige Veröffentlichung wissenschaftlicher Daten;

4. Produktentwickler:innen sind aufgefordert, ihre Covid-19-Technologien, geistigen Eigentumsrechte und Daten freiwillig in den Patentpool einzubringen, um eine schnelle und kostengünstige Generikaproduktion zu ermöglichen;

5. Offene Innovationsmodelle und Technologietransfer zu fördern, um eine lokale Produktion zu ermöglichen und lokale Versorgungsstrukturen zu stärken.

Zum Vorbild nimmt sich C-TAP den *Medicines Patent Pool*[13], der große Erfolge in der günstigen Verfügbarkeit von Medikamenten zur Behandlung von HIV, Tuberkulose und Hepatitis C gebracht hat. Auch dem C-TAP verweigert die deutsche Bundesregierung übrigens die Unterstützung. Es fehlt bisher an der Beteiligung von Industriestaaten und Unternehmen, um den Pool auch mit nutzbarem Inhalt zu füllen.

Der *COVID-19 mRNA vaccine technology transfer hub* ist im April 2021 mit speziellem Fokus auf die mRNA-Wirkstoffe ins Leben gerufen worden.

Weitere Argumente fasst Cooperate Europe hier[14] zusammen.

Frage: Wieso hilft die Aussetzung von Patenten bei der COVID-Impfung, obwohl auf den COVID-Impfstoffen [zum Teil] noch gar keine Patente liegen, weil der Patentprozess bei den Impfstoffen noch gar nicht abgeschlossen ist (alle im Anmeldestadium, wenn überhaupt)?

Antwort: Der Patentschutz auf ein Produkt oder eine Technologie beginnt nicht an dem Tag, an dem das Patent gewährt wird, sondern i. d. R. rückwirkend zu dem Tag, an dem das Patent angemeldet wurde. Die rechtlichen Details sind in jedem Land unterschiedlich, was die Sache komplex macht. Grundsätzlich ist es aber ohne Zweifel, dass Patente den Zugang zu Medikamenten im globalen Süden behindern. Das wird regelmäßig von anerkannten humanitären Hilfsorganisationen wie *Ärzte ohne Grenzen* attestiert. Auch bei anderen Impfstoffen waren Patente historisch oft ein Hindernis bei der schnellen und fairen Verteilung.

Außerdem bezieht sich der TRIPS-Waiver auf verschiedene Arzneimittel und Technologien – also nicht nur auf Impfstoffe, die zum Kampf gegen die Pandemie nötig sind. Darunter sind auch Produkte, die bereits abgeschlossene Patentverfahren hinter sich haben.

Frage: Patentiert sind z. B. einige Grundlagentechnologien für mRNA-Impfstoffe, diese werden aber nicht nur für Corona-Impfstoffe eingesetzt. Würde ein Aussetzen der Patente dann alle diese Impfstoffe betreffen?

Antwort: Prinzipiell ist der TRIPS-Waiver explizit zeitlich auf die Dauer der Pandemie begrenzt. Unabhängig davon, welche konkreten Patente bzw. welches geistige Eigentum betroffen wäre, besteht also keine Gefahr, dass plötzlich Grundlagentechnologien nicht mehr patentiert wären.

Frage: Wäre es nicht besser, die reicheren und produzierenden Länder zu verpflichten, Mittel (finanziell und organisatorisch)

bereitzustellen, um trotz evtl. bestehender Patente Impfstoff und Impfkapazität in die ärmeren Länder zu bringen?

Antwort: Diesen Ansatz verfolgt COVAX – jedoch ohne bindende Verpflichtungen. Und selbst die überschaubaren Ziele der COVAX-Initiative werden aktuell weit verfehlt. Von den 700 Millionen global produzierten Dosen sind nur 0,2 % in Ländern mit niedrigen Einkommen verimpft worden. (Stand Anfang April[15]). In Anbetracht von „Impfnationalismus", wie ihn die WHO konstatiert, ist leider nicht damit zu rechnen, dass freiwillige Selbstverpflichtungen dazu führen, dass Länder Impfdosen in signifikanten Mengen in den globalen Süden schicken werden.

Die momentanen Impfstoffproduktionskapazitäten liegen bei 3,5 Milliarden jährlichen Dosen. Um 70 % der Weltbevölkerung zu impfen und damit Herdenimmunität zu erreichen, benötigen wir etwa 11-15 Milliarden Impfdosen. Die vorhandenen Produktionskapazitäten reichen also bei weitem nicht aus, und es müssen neue Kapazitäten erschlossen werden. Gerade dann ist es gesundheitspolitisch nicht sinnvoll, auch weiterhin pharmakologische Produktionskapazitäten nur im globalen Norden aufzubauen. Im Sinne einer globalen Resilienz gegen Pandemien ist es wichtig, diese Abhängigkeitsbeziehungen zwischen Industrienationen und Schwellenländern zu reduzieren. Dies gelingt durch den Aufbau und die Nutzung von Produktionskapazitäten und durch Wissenstransfer. Dies ist umso gewichtiger, da die Gefahr neuer Pandemien durch Bevölkerungswachstum und Klimawandel stetig zunimmt.

Frage: Warum sollen private Unternehmen/Konzerne die finanzielle Last einer evtl. Patentfreigabe schultern, die vermutlich über die gewährten Staatshilfen hinausgeht? Ist es gerechtfertigt, Einbußen in nicht bezifferter Höhe zu verlangen? Könnte es evtl. eine sinnvolle Forderung sein, den Verzicht auf Einnahmen wegen Freigabe der Patente auf einen prozentual von der Gewährung öffentlicher Gelder abhängigen Betrag zu begrenzen? Gibt es aus eurer Sicht keinerlei Unterschied zwischen Pharmariesen und relativ kleinen Produzenten wie Biontech?

Antwort: Diese Unternehmen machen aktuell zum Teil Rekord-Gewinne, die durch weitreichende Unterstützung durch öffentliche Gelder überhaupt erst möglich geworden sind. Auch ist überhaupt nicht klar, ob infolge des TRIPS-Waiver überhaupt Gewinne verloren gehen werden. Schließlich geht es darum, zusätzliche Impfstoffdosen in und für Länder zu produzieren, die zum jetzigen Zeitpunkt nicht oder nur sehr unzureichend beliefert werden. Der TRIPS-Waiver führt dazu, dass Patentverletzungen auf globaler Ebene vorübergehend nicht verfolgt werden. Jedes Land kann jedoch entscheiden, auf nationaler oder polynationaler Ebene Patentrechte weiter zu verfolgen – innerhalb Deutschlands braucht Biontech also keine Konkurrenz zu befürchten. Weiterhin entscheidet jedes Land selbst, welchen Produkten sie die Zulassung erteilt. Und schließlich ist es wichtig zu verstehen, dass der Corona-Impfstoffmarkt alles andere als gesättigt ist. Es fehlen akut Impfdosen. Im globalen Norden – dem Absatzmarkt von Biontech – braucht die Firma also keine Verdrängung befürchten, da genug weitere Schutzmechanismen greifen.

Im Übrigen: Biontech kooperiert mit Pfizer – einem absoluten Pharmariesen. Wobei letztlich die Größe dieser Firmen aber von keinerlei praktischer Bedeutung ist. Es bleibt am Ende die Frage, wie viele Menschenleben der Gesellschaft und der deutschen Bundesregierung die Gewinne dieser Unternehmen wert sind.

Frage: Wie war *konkret* die Regelung der zitierten HIV/AIDS-Impfstofffreigabe?

Die Kurzfassung: Die Hersteller wurden gezwungen, den Ländern des globalen Südens Lizenzvereinbarungen für gewisse Medikamente anzubieten oder ihnen werden die Patente aberkannt.[16,17]

Frage: Welchen Anteil an den Gesamtentwicklungskosten stellen die 375 Millionen EUR dar, mit denen Biontech gefördert wurde?

Antwort: Laut Biontech-Geschäftsbericht von 2019 hat die Firma 225 Millionen Dollar in einer Series B Investitionsrunde und weitere 149 Millionen im Rahmen des Börsengangs eingesammelt. Laut Biontech-Geschäftsbericht für die ersten neun Monate 2020 beliefen sich die Forschungsausgaben der gesamten Firma auf 388 Millionen Euro[18], also geringfügig mehr als die öffentliche Förderung. Welcher Anteil davon konkret in die Entwicklung der Covid-Impfstoffe geflossen ist, ist keine öffentlich zugängliche Information. Ebenfalls unbekannt sind die tatsächlichen Produktionskosten einer Dosis. Sollte Biontech die 300 Millionen vertraglich vereinbarten Dosen an die EU liefern, läge der Umsatz – allein in der EU – bei etwa 6 Milliarden Euro. Allein im ersten Quartal 2021 hat Biontech einen Gewinn von 1,1 Milliarden Euro eingefahren[19]. Morgan Stanley projiziert Biontech/Pfizer einen weltweiten Umsatz durch den Impfstoff von 13 Milliarden Euro in 2021[20].

Verhandlungen zwischen EU und Biontech liefen zu großen Teilen geheim ab, Verträge wurden nicht oder nur geschwärzt veröffentlicht. Dass der ursprünglich geforderte Preis pro Dosis mehr als doppelt so hoch war als das, was am Ende wohl verhandelt wurde, zeigt, dass hier knallharte Profitinteressen im Vordergrund stehen[21]. Eine wichtige und oft genannte Forderung von Aktivist:innen (neben dem TRIPS-Waiver) ist daher, dass Pharmaunternehmen zu mehr Transparenz verpflichtet werden müssen, wenn sie öffentliche Gelder erhalten.

Frage: Warum ist es der richtige Weg, Staaten, die vielfach selbst einen hohen Korruptionsfaktor aufweisen[22], einseitig zu gestatten, Eigentumsrechte zu ignorieren? Wie verhindert man einen Dammbruch für Patentrechte generell?

Antwort: Sofern ein Land einen hohen Korruptionsfaktor aufweist, wird die Korruption einer fairen Verteilung im Wege stehen, unabhängig davon, wer die Impfstoffe produziert. Zudem: Eigentumsrechte werden nicht ignoriert. Die internationale Durchsetzung dieser Rechte wird zeitlich begrenzt ausgesetzt. Im Anschluss greifen dieselben Mechanismen wie bisher.

Frage: Mit welcher konkreten Begründung hat die Bundesregierung/EU sich gegen die Annahme des TRIPS-Waivers ausgesprochen?

Antwort: Die Argumente lassen sich zusammenfassen als:

- TRIPS-Waiver seien ineffektiv und nicht zielführend
- TRIPS-Flexibilitäten + COVAX würden ausreichen
- Forschung ist risikobehaftet und kostet Geld – Patente aussetzen bremst Innovation
- der Wirtschaftsstandort Deutschland muss geschützt werden

Weitere Details hier[23].

Valdis Dombrovskis, geschäftsführender Vizepräsident und Kommissar für Wirtschaft und Kapitaldienstleistungen der EU-Kommission hat in einer Rede vom 14. April 2021 die offizielle Position der EU umrissen. Eine gute, kommentierte Version dieser Rede findet sich hier[24].

Frage: Indien, eines der beiden Länder, die den TRIPS-Waiver auf den Weg gebracht haben, ist Heimat des größten Impfstoffproduzenten der Welt, des Serum Institute of India (SII), der unter anderem große Mengen des AstraZaneca-Impfstoff herstellt und diese zumindest in Indien für sehr moderate Preise verkauft. Da Indien möglicherweise noch weitere Kapazitäten aufbauen kann, steckt dahinter durchaus auch ein wirtschaftliches Interesse. Ähnliches dürfte auch für Südafrika gelten, wo es unausgelastete Produktionskapazitäten gibt. Zudem hat die indische Regierung schon seit längerem Covid-19-Impfstoffexporte aus Indien untersagt.

Antwort: Zunächst zu dem Punkt, dass Indien die Impfstoff-Exporte gestoppt hat: Seit Ende Januar kann die EU Lieferanten, die Lieferverpflichtungen für die EU haben, Ausfuhrgenehmigungen für in der EU produzierte Impfstoffe verweigern und hat davon auch schon Gebrauch gemacht – nur weil vertraglich vereinbarte Mengen nicht erzielt wurden, und das, obwohl viele EU-Länder die bereits gelieferten Dosen noch längst nicht verimpft hatten. Die USA hat bisher fast gar keinen Impfstoff exportiert. Dagegen ist die in Indien aktuell stark reduzierte Ausfuhr (es werden weiterhin kleinere Spenden verteilt und auch weiterhin langsam an COVAX geliefert) eine direkte Reaktion auf die aktuelle dramatische Situation in Indien.

Tatsächlich ist Indien unter den Spitzenreitern, die weltweit die meisten Impfdosen exportiert haben – bisher über 66 Millionen[25], darunter 28 Millionen für COVAX. Darüber hinaus ist Indien nach China auf Platz zwei der meisten gespendeten Dosen (> 9 Millionen, mehr als ein Drittel der gespendeten Gesamtmenge).

Dass auch Indien und Südafrika wirtschaftliche Interessen vertreten, mag stimmen. Der zentrale humanitäre Gesichtspunkt an dieser Stelle ist aber, dass so schnell, so viel und so günstig wie möglich Impfstoff produziert werden muss. Die in der Frage angesprochenen unausgelasteten Produktionskapazitäten sind eine verschenkte Chance, die Pandemie zu verkürzen. Indien ist offenbar in der Lage und gewillt, sehr viel Impfstoff zu vergleichsweise günstigen Preisen herzustellen und diesen zu exportieren – das halten wir für unterstützenswert! Und genau hier ist ein Vorteil vom TRIPS-Waiver gegenüber den Lizenzen, die es momentan nur dem SII erlauben Astra Zeneca herzustellen, wobei das Wissen ja nun nachweislich im Land ist und auf weitere Produktionsstätten ausgeweitet werden könnte.

Um eine ähnliche Entwicklung auch in anderen Schwellenländern zu ermöglichen, braucht es Initiativen wie den TRIPS-Waiver und geeignete Formen des Technologietransfers.

Anmerkungen

1 *https://www.fiff.de/presse/ImpfstoffeFreigeben*
2 *https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/IP/C/W669.pdf&Open=True*
3 *https://www.fiff.de/presse/ImpfstoffeFreigebenFAQ*
4 *https://www.fiff.de/presse/ImpfstoffeFreigeben*
5 *https://www.aerzte-ohne-grenzen.de/faq/1927*
6 *https://www.aerzte-ohne-grenzen.de/presse/europa-covid-19-impfstoff-engpass*
7 *https://www.who.int/director-general/speeches/detail/director-general-s-opening-remarks-at-the-media-briefing-on-covid-19-9-april-2021*
8 *https://healthpolicy-watch.news/views-from-a-vaccine-manufacturer-qa-abdul-muktadir-incepta-pharmaceuticals/, https://theintercept.com/2021/04/29/covid-vaccine-factory-production-ip/, https://www.mabxience.com/mabxience-enters-into-an-agreement-with-astra-zeneca-to-produce-covid-19-vaccine/*
9 *https://www.fiff.de/presse/ImpfstoffeFreigeben*
10 *https://youtu.be/86F-nFkskPs?t=4577*
11 *https://www.who.int/news/item/29-05-2020-international-community-rallies-to-support-open-research-and-science-to-fight-covid-19*
12 *https://www.who.int/news-room/articles-detail/establishment-of-a-covid-19-mrna-vaccine-technology-transfer-hub-to-scale-up-global-manufacturing*
13 *https://medicinespatentpool.org/partners/mpp_global_manufacturers_open_pledge/*
14 *https://corporateeurope.org/en/2021/04/big-pharma-lobbys-self-serving-claims-block-global-access-vaccines*
15 *https://www.who.int/director-general/speeches/detail/director-general-s-opening-remarks-at-the-media-briefing-on-covid-19-9-april-2021)*
16 *https://www.healthaffairs.org/doi/10.1377/hlthaff.2018.05391*
17 *https://www.wto.org/english/res_e/booksp_e/ddec_e.pdf*
18 *https://www.wiwo.de/unternehmen/dienstleister/impfstoff-entwickler-biontech-mit-hohen-verlusten-aber-deal-mit-eu/26610220.html*
19 *https://www.rnd.de/wirtschaft/biontech-1-1-milliarden-euro-gewinn-im-ersten-quartal-2021-STBKXC2WVRLRGQEYKWVVIEIZ6E.html*
20 *https://www.theguardian.com/business/2020/nov/10/pfizer-and-biontech-could-make-13bn-from-coronavirus-vaccine*
21 *https://www.tagesschau.de/investigativ/ndr-wdr/corona-impfstoff-biontech-105.html*
22 *https://www.transparency.de/cpi/?L=0)*
23 *https://dip21.bundestag.de/dip21/btd/19/278/1927862.pdf*
24 *https://msfaccess.org/sites/default/files/2021-04/COVID_NoCountry_SpeechWTO_NoAuthor_2021_MSB71190_1081px.png*
25 *https://www.mea.gov.in/vaccine-supply.htm*

Hans-Jörg Kreowski, Wolfgang Krieger

Künstliche Intelligenz – „künstlich“ ja, „Intelligenz“ wohl kaum

Dieser Artikel ist eine um etwa ein Drittel gekürzte und leicht modifizierte Fassung eines Essays, das in dem von Anna Strasser, Wolfgang Sohst, Ralf Stapelfeldt, Katja Stepec herausgegebenen Sammelband Künstliche Intelligenz – Die große Verheißung *erschienen ist (MoMo Berlin, Philosophische KonTexte 8, xenomoi Verlag, Berlin 2021, S. 259 – 278). Die Kürzung betrifft vor allem eine Skizze der kurzen Geschichte der Künstlichen Intelligenz und ihre Einbettung in den Kontext der Industrialisierung. Wir danken dem xenomoi-Verlag für die freundliche Erteilung der Nachdruckgenehmigung.*

Die Künstliche Intelligenz (KI) wurde 1956 von einigen jungen Wissenschaftlern in den USA als Teilgebiet der Informatik gegründet (siehe McCarthy et al. 1955). Erklärtes Ziel war, Computersysteme zu entwickeln, die in zunehmendem Maße Merkmale menschlicher Intelligenz nachbilden, wie logisches Schließen, Planen, Lernen, Textverstehen und anderes mehr. Die Ziele – und auch die in der KI favorisierten Methoden – haben sich seitdem gar nicht allzu sehr verändert. In den letzten Jahren aber verzeichnet die KI durch die erreichte Rechengeschwindigkeit und Speicherkapazität bemerkenswerte technologische Erfolge beispielsweise bei der weltmeisterlichen Beherrschung von Spielen wie Schach und Go oder bei dem erfolgreichen Einsatz der wesentlich anwendungsorientierten Sprach- und Bildverarbeitung.

Dadurch hat die KI einschließlich der Robotik in den letzten Jahren in Wirtschaft, Politik und der medialen Öffentlichkeit eine Aufmerksamkeit erreicht, wie sie wissenschaftlichen und technologischen Gebieten selten zuteil wird. Neben einer Flut von Zeitungs- und Zeitschriftenartikeln sowie zahlreichen Radio- und Fernsehbeiträgen ist allein die Zahl der erschienenen populärwissenschaftlichen Sachbücher eindrucksvoll. Als kleine Auswahl seien erwähnt Nick Bostroms *Superintelligenz – Paths, Dangers, Strategies* von 2014, der von John Brockman 2017 herausgegebene Band *Was sollen wir von KI halten – Die führenden Wissenschaftler unserer Zeit über intelligente Maschinen*, Olle Hägströms *Here be Dragons – Science, Technology and the Future of Humanity* und Yuval Noah Hararis *Homo deus: eine Geschichte von Morgen,* beide aus dem Jahre 2017, Yvonne Hofstetters *Sie wissen alles: Wie intelligente Maschinen in unser Leben eindringen und warum wir um unsere Freiheit kämpfen müssen* von 2014, Jerry Kaplans *Künstliche Intelligenz – Eine Einführung* aus dem Jahre 2017, Ray Kurzweils *How to Create Mind – The Secrets of Human Thoughts Revealed*, erschienen 2012, Kai-Fu Lees *AI Superpowers – China, Silicon Valley und die neue Weltordnung* von 2019, Richard David Prechts *Künstliche Intelligenz und der Sinn des Lebens* aus dem vorigen Jahr sowie Tony Walshs *It's Alive – Wie Künstliche Intelligenz unser Leben verändern wird* aus dem Jahre 2018. Die Autorinnen und Autoren setzen sich mit den zu erwartenden gesellschaftlichen Auswirkungen auf die Arbeitswelt, Produktion, Verwaltung, Bildung, Wissenschaft, Polizei und Militär auseinander und diskutieren die Gefahren intensivierter sozialer Überwachung.

Ein Hauptthema ist auch *Superintelligenz*, d. h. die Frage nach einem KI-System, das die menschliche Intelligenz übertrifft. In der KI haben sich frühzeitig zwei Fraktionen herausgebildet. Die Vertreterinnen und Vertreter der sogenannten schwachen KI streben informationsverarbeitende Systeme an, die einzelne Leistungen simulieren, für die Menschen ihre Intelligenz einsetzen. Die viel kleinere Gruppe von Anhängerinnen und Anhängern der starken beziehungsweise allgemeinen KI dagegen propagieren Systeme, die selbst intelligent sind bis hin zur Superintelligenz. Insbesondere gegen die Positionen und bis heute unerfüllten – vielleicht sogar unerfüllbaren – Versprechen der starken KI regte sich frühzeitig Kritik. Siehe dazu beispielsweise die Bücher *Industrieroboter. Zur Archäologie der zweiten Schöpfung* von Wolfgang Coy aus dem Jahre 1988, *Was Computer nicht können – Die Grenzen künstlicher Intelligenz* von Hubert L. Dreyfus von 1989 sowie *Computer Power and Human Reason* von Joseph Weizenbaum, erschienen 1976.

Angesichts der technologischen Erfolge der KI setzen Wirtschaft und Politik ihre Hoffnungen und Erwartungen in die KI als Schlüsseltechnologie der Zukunft. Um dieses Ziel zu erreichen, werden weltweit Aberhunderte Milliarden US-Dollar in die Förderung von KI investiert. In diesem Artikel wollen wir der Frage nachgehen, was es mit diesem Hype um die KI auf sich hat. Wo liegen die technologischen Potentiale von KI und Robotik? Sind die an die KI geknüpften Erwartungen gerechtfertigt oder übertrieben? Welche Risiken sind mit dem ungebremsten Einsatz von KI verbunden? Was hat es überhaupt mit der ‚Intelligenz‘ in Künstlicher Intelligenz auf sich?

Abschnitt 1 ist dem aktuellen Hype um die KI gewidmet, in Abschnitt 2 werden natürliche und künstliche Intelligenz gegenübergestellt, und Abschnitt 3 beschließt diesen Artikel mit einer vorläufigen Bilanz.

1 Der aktuelle Hype um KI im Zusammenspiel von Politik, Wirtschaft und Wissenschaft

Es gibt seit einigen Jahren einen riesigen Hype um die Künstliche Intelligenz. Die unbestreitbaren wissenschaftlichen und technologischen Erfolge haben weltweit bei Politik und Wirtschaft hohe Erwartungen geweckt. In nahezu allen gesellschaftlichen Bereichen von Produktion, Dienstleistung, Transport und Verkehr über Verwaltung, Medizin, Bildung und Wissenschaft bis hin zum staatlichen Handeln einschließlich Polizei und Militär werden bahnbrechende Fortschritte prognostiziert. Mit dem Hinweis auf die exorbitanten Fördermittel wird dieser Aspekt in 1.1 etwas ausgeführt. Es ist allerdings noch keineswegs gesichert, dass alle diese Blütenträume insbesondere in der Politik reifen, was in 1.2 aufgegriffen wird. Man darf davon ausgehen, dass die aktuellen Entwicklungen im Bereich der Künstlichen Intelligenz und der Robotik vielfältige Chancen eröffnen, aber auch erhebliche Risiken bergen wie die Vernichtung von Arbeits-

plätzen, neue Formen der sozialen Überwachung und neue Arten perfider Waffensysteme.

1.1 Umfangreiche staatliche Förderung

Klar ist jedenfalls, dass einiges passieren wird. Denn es wird in den kommenden Jahren unglaublich viel Geld – umgerechnet Hunderte von Milliarden US-Dollar – in die Entwicklung der Künstlichen Intelligenz gesteckt. Viele Länder der Welt sowie die Europäische Union haben KI-Strategien formuliert, um den Anschluss nicht zu verlieren, um die künftige Wertschöpfung zu garantieren, um führend zu sein oder zu bleiben, um in einem – möglicherweise nur eingebildeten – geostrategischen Rennen die Nase vorn zu haben. Interessanterweise wird dabei oft darauf verwiesen, dass nicht nur die Chancen zum Wohle der Menschen genutzt, sondern auch die Risiken vermieden und ethische Grundsätze eingehalten werden sollen. Es würde den Rahmen sprengen, sich mit den verschiedenen Strategiekonzepten auseinanderzusetzen (siehe z. B. den Artikel (Harloff et al. 2018) zur deutschen Strategie mit vielen Hinweisen auf die Strategie anderer Länder). Als typisches Beispiel soll aber auf die Strategie *Künstliche Intelligenz* der Bundesregierung (Stand: November 2018) etwas näher eingegangen werden, die auf 47 Seiten einen detaillierten Rundumschlag macht, welche Bereiche wie von KI profitieren sollen. Die erklärten Ziele sind der Ausbau der „Wettbewerbsfähigkeit der deutschen Wirtschaft" und ein „spürbarer gesellschaftlicher Fortschritt". In der Zusammenfassung *AI made in Germany* kann man da lesen:

> *„Die Bundesregierung wird den Gestaltungsauftrag, der sich aus den raschen Fortschritten im Bereich der Künstlichen Intelligenz ergibt, annehmen und den Innovationsschub, der mit der Technologie einhergeht, zum Wohle aller umfassend nutzen. Wir wollen den exzellenten Forschungsstandort Deutschland sichern, die Wettbewerbsfähigkeit der deutschen Wirtschaft ausbauen und die vielfältigen Anwendungsmöglichkeiten von KI in allen Bereichen der Gesellschaft im Sinne eines spürbaren gesellschaftlichen Fortschritts und im Interesse der Bürgerinnen und Bürger fördern. Wir werden dabei den Nutzen für Mensch und Umwelt in den Mittelpunkt stellen und den intensiven Austausch mit allen gesellschaftlichen Gruppen fortsetzen. Deutschland ist in vielen Bereichen der Künstlichen Intelligenz bereits heute ausgezeichnet aufgestellt. Diese Strategie greift bestehende Stärken auf und überträgt sie in Bereiche mit noch nicht oder wenig ausgeschöpften Potenzialen." (Die Bundesregierung 2018, S. 6).*

Ansonsten besteht die Strategie überwiegend aus einer langen Liste an Wünschen und Absichten, die fast alle mit „Wir werden …" oder „Die Bundesregierung wird …" beginnen. So sollen Deutschland und Europa ein führender KI-Standort werden zur Sicherung künftiger Wettbewerbsfähigkeit. Dafür sollen bestehenden Kompetenzzentren für KI-Forschung und weitere einzurichtende Zentren zu einem nationalen Netzwerk von mindestens zwölf Zentren und Anwendungshubs ausgebaut werden, verbunden mit der Schaffung von mindestens 100 neuen KI-Professuren. Außerdem sind der Aufbau eines deutsch-französischen Forschungs- und Innovationsnetzwerkes, ein europäisches Innovationscluster zu KI, die KI-spezifische Unterstützung von mittelständischen Unternehmen durch ein Kompetenzzentrum Mittelstand 4.0, die Unterstützung von Existenzgründungen und Förderung im Bereich Wagniskapital sowie der Aufbau einer vertrauenswürdigen Daten- und Analyseinfrastruktur geplant. Als weiteres großes Ziel wird „eine verantwortungsvolle und gemeinwohlorientierte Entwicklung und Nutzung von KI" (Seite 9) formuliert. Es soll erreicht werden durch die Einrichtung eines deutschen Observatoriums für Künstliche Intelligenz, durch die Organisation eines europäischen und transatlantischen Dialogs zum menschenzentrierten Einsatz von KI in der Arbeitswelt, durch eine Nationale Weiterbildungsstrategie zur Förderung der Kompetenzen von Erwerbstätigen im Hinblick auf den digitalen Wandel und neue Technologien wie KI, durch die Sicherung betrieblicher Mitbestimmungsmöglichkeiten bei der Einführung und Anwendung von KI und von der Förderung von KI-Anwendungen zum Nutzen von Umwelt und Klima, wobei „50 Leuchtturmanwendungen" (Seite 7) angestoßen werden sollen. Als drittes großes Ziel ist genannt, „im Rahmen eines breiten gesellschaftlichen Dialogs und einer aktiven politischen Gestaltung KI ethisch, rechtlich, kulturell und institutionell in die Gesellschaft ein(zu)betten" (Seite 8). Dafür soll ein Runder Tisch mit Datenschutzbeauftragten und Wirtschaftsverbänden für Datenschutzrechtskonformität von KI-Systemen sorgen. Dafür soll „die Entwicklung von innovativen Anwendungen, die die Selbstbestimmung, die soziale und kulturelle Teilhabe sowie den Schutz der Privatsphäre der Bürgerinnen und Bürger unterstützen" (Seite 8), gefördert werden. Schließlich ist eine KI-Plattform vorgesehen, „in welcher ein Austausch zwischen Politik, Wissenschaft und Wirtschaft mit der Zivilgesellschaft organisiert wird" (Seite 7). Die einzelnen Maßnahmen mögen gut klingen, insgesamt handelt es sich aber eher um einen Gemischtwarenladen. Es ist schwer vorstellbar, dass die Umsetzung aller dieser Einzelziele in einem systematischen Prozess organisiert werden kann.

Die KI-Strategie ist der Bundesregierung nur vergleichsweise bescheidene 3 Milliarden Euro für sieben Jahre bis 2025 wert, während die Volksrepublik China im gleichen Zeitraum wohl 150 Milliarden ausgeben will und in den USA staatlich und privatwirtschaftlich ohnehin jährlich mehr als der zehn- oder zwanzigfache Betrag investiert wird. Die Strategie ist Ausfluss eines langen Planungs-, Kommunikations- und Beratungsprozesses zwischen Politik, Wirtschaft und Wissenschaft, wobei die letzten beiden Parteien nicht völlig uneigennützig agiert haben, sondern eher so, dass sie ein möglichst großes Stück vom Kuchen abbekommen. Die Erfahrungen mit der immensen staatlichen Förderung durch Drittmittel in Deutschland und der Europäischen Union für diverse wissenschaftliche Disziplinen, aber insbesondere auch für Informatik und Informationstechnik zeigen, dass den Prognosen und Versprechungen von Wirtschaft und Wissenschaft hinsichtlich der Zeitperspektiven und der tatsächlichen technologischen Umsetzbarkeit von Forschungs- und Entwicklungsprojekten wenig Glauben geschenkt werden darf.

1.2 Politische Wunschträume

Zum Schuljahresbeginn 2017 ist der russische Präsident Wladimir Putin in einer via Satellit live übertragenen Unterrichtsstunde zum Motto *Zukunftsorientiertes Russland* vor fast einer Millio-

nen Schülerinnen und Schüler laut Epoch Times auf die Künstlichen Intelligenz eingegangen:

> *„In der Künstlichen Intelligenz liege die Zukunft Russlands und die der Menschheit … Und wer in diesem Bereich die Führungsrolle übernimmt, werde die ganze Welt beherrschen … In ihr liegen kolossale Möglichkeiten, aber auch Bedrohungen, die heute schwer vorherzusagen sind … Deswegen würde er es nicht gerne sehen, dass jemand eine Monopolstellung in KI-Technologien genießt … Sollte Russland die Führungsposition in der Entwicklung künstlicher Intelligenz einnehmen, werde es sein Wissen mit anderen Ländern teilen, wie es das bereits in der Kerntechnik tut …" (Epoch Times 2017)*

Die ehemalige Staatssekretärin im Verteidigungsministerium Katrin Suder hat ganz Ähnliches gesagt und in diversen KI-Strategien liest es sich zumindest zwischen den Zeilen nicht viel anders. Der Wettlauf um die Führung auf dem Gebiet der KI ist allerdings kein Marathonlauf mit einer Siegerin oder einem Sieger. Die USA und China werden schon wegen des Investitionsumfangs eine Marktführerschaft erreichen, aber Europa, Japan, Russland und auch kleinere Länder werden ihre Nischen finden. Und wie man am Beispiel der USA sehen kann, ist wirtschaftliche Stärke kein Garant für politische Vormacht.

2 Künstliche Intelligenz und natürliche Intelligenz – (k)ein Vergleich

Eine künstliche Blume ist keine Blume, sieht allenfalls so aus, riecht vielleicht sogar so. Ein künstlicher See ist ein See, nur nicht natürlich entstanden. Von welcher Art ist das ‚Künstlich' in Künstlicher Intelligenz? Ob Künstliche Intelligenz algorithmische Aufgaben erledigt, für die Menschen ihre Intelligenz einsetzen, und damit eher der künstlichen Blume ähnelt oder ob sie echte Intelligenz verwirklicht, nur wie der künstliche See künstlich hergestellt, ist in dem Fachgebiet umstritten, und die Fachleute sind sich überhaupt nicht einig. Da allerdings die Wirkprinzipien menschlicher Intelligenz weitgehend ungeklärt sind, wäre es höchst verwunderlich, wenn Künstliche Intelligenz so intelligent wäre wie die Macherinnen und Macher der KI-Systeme. Um diese Einschätzung zu untermauern, wird in 2.1 dem Phänomen natürlicher Intelligenz nachgegangen, in 2.2 der algorithmische Rahmen Künstlicher Intelligenz skizziert und in 2.3 eine – zugegebenermaßen sehr vorläufige – vergleichende Betrachtung angestellt.

2.1 Natürliche Intelligenz

Natürliche Intelligenz, wie sie vor allem Menschen zugeschrieben wird, mittlerweile aber auch anderen Lebewesen, teils sogar Pflanzen, ist ein Phänomen, das sich in vielen Beispielen zeigt, aber bisher nicht genau definiert werden kann – vielleicht sogar gar nicht genau definierbar ist. Die Intelligenz eines Menschen ist vor allem eine Leistung seines Gehirns, die es ohne Verbindung zu den Sinnesorganen und dem Versorgungssystem des Körpers aber auch nicht gäbe. Darüber hinaus ist Intelligenz nicht sauber von anderen Leistungen des Gehirns zu trennen. Ein Mensch kann nicht nur denken, lernen, sprechen, lesen, schreiben und rechnen, sondern auch glauben, hoffen, zweifeln, lieben und hassen. Ein Mensch kann intelligent sein – und kreativ, phantasievoll, einfühlsam, naiv, faul, dumm und grausam. Rationalität ist mit Irrationalität gepaart, Klugheit mit Torheit, Freundlichkeit mit Abneigung, Interesse mit Ignoranz. Es ist unbekannt, wie diese Leistungen im Gehirn zustande kommen, wie sie zusammenhängen und sich vielleicht sogar bedingen. Kognitionswissenschaft, Hirnforschung, Psychologie, Medizin und Biologie haben in den letzten Jahren große Fortschritte gemacht, aber vieles, was sich im Gehirn abspielt, bleibt ein Rätsel (siehe dazu beispielsweise die Streitschrift von Felix Hasler (2012)). Niemand kann bisher sagen, wie ein einzelner Gedanke geformt wird. Vieles lässt sich als intelligent benennen, aber ein vollständiges und präzises Verständnis von Intelligenz ist ein Ziel der Wissenschaft, das immer noch in weiter Ferne liegt, wenn es sich überhaupt erreichen lässt.

Menschliche Intelligenz bringt nicht nur individuell Erstaunliches zustande, sondern hat vor allem auch eine gesellschaftliche Dimension. Die Menschheit hat in den letzten zehntausend Jahren – und auch schon davor – phantastische Leistungen hervorgebracht in Ackerbau, Viehzucht, Städtebau, Metallverarbeitung, Schrift, Literatur, Musik, Kunst, was immer auch mit Kehrseiten wie Unterdrückung, Ausbeutung, Sklaverei, Krieg, Teilung in Arm und Reich und in Mächtige und Ohnmächtige verbunden war. Ohne menschliche Intelligenz wären solche gesellschaftlichen Entwicklungen unmöglich.

2.2 Künstliche Intelligenz

Bei der KI verhält es sich völlig anders. KI ist ein Teilgebiet der Informatik, in der es um Methoden, Gesetzmäßigkeiten und Anwendungen von Daten- und Informationsverarbeitung im weitesten Sinne geht, wobei unter Verarbeitung die maschinelle Ausführung verstanden wird. Insbesondere ist an Computer gedacht und an Programme und Algorithmen, die auf Computern laufen. Anders und kurz gesagt, geht es um „Berechenbarkeit". Und zu den Möglichkeiten und Grenzen der Berechenbarkeit gibt es in der Informatik eine Reihe von Einsichten, die auf ein breites Einverständnis im Fach stoßen und an denen auch die KI nicht vorbeikommt.

Bereits 1937 hat Alan M. Turing in seinem Aufsatz *On Computable Numbers, with an Application to the Entscheidungsproblem* (Turing 1937) das Konzept der Berechenbarkeit präzise gefasst, was als Turingsche These bezeichnet wird: Alles, was berechenbar ist, lässt sich von einer Turing-Maschine ausführen. Nach dem Vorbild eines Büroangestellten ist eine Turing-Maschine ein sehr vereinfachtes Computer-Modell. Sie führt Arbeitsschritte auf „Zeichenketten" – also auf Texten, Zahlenkolonnen u. ä. – aus, wobei in einem Schritt ein Zeichen gelesen wird, an dieser Stelle ein neues Zeichen geschrieben werden kann und dann an derselben Stelle oder links oder rechts davon weitergearbeitet wird. Die Turing-Maschine befindet sich immer in einem von endlich vielen Zuständen. Ihre Arbeit erfolgt nach einem „Programm", das aus endlich vielen Instruktionen besteht, wobei eine Instruktion für einen aktuellen Zustand und das aktuell gelesene Zeichen festlegt, welcher Folgezustand eingenommen, welches Zeichen geschrieben und wo weiterge-

arbeitet wird. Beginnend mit einer Eingabe-Zeichenkette und einem Anfangszustand, besteht eine Berechnung der Turing-Maschinen dann aus einer Folge von Schritten gemäß den Instruktionen, bis ein Endzustand erreicht ist. Das klingt alles recht harmlos und mag vage an die Arbeit existierender Computer erinnern. Das Konzept erlangt seine Mächtigkeit dadurch, dass die bearbeitete Zeichenkette beliebig verlängert werden kann und dass nicht jede Berechnung in einem Haltezustand enden muss, sondern auch unendlich fortlaufen kann.

Da die Voraussetzung der Turingschen These ‚Alles, was berechenbar ist´ nicht formalisiert werden kann, ist die These ein Glaubenssatz nach der Art der Relativitätstheorie, die postuliert, dass nichts schneller ist als Licht. Es gibt jedoch Hunderte, wenn nicht Tausende Indizien, die die These stützen. So sind alle bekannten Computermodelle (einschließlich DNA-Computer und Quantencomputer) und alle bekannten Programmierungsparadigmen wie imperative, logische, rekursive, funktionale Programmierung gleichwertig zu Turing-Maschinen, was die Berechnungsfähigkeit angeht. Und es gibt bisher nichts Ernstzunehmendes, was gegen die These spricht. Setzt man die Turingsche These als richtig voraus, zieht das einige Grenzen der Berechenbarkeit nach sich. So lassen sich viele Datenverarbeitungsprobleme formulieren, die nicht berechenbar sind. So lassen sich die berechenbaren Probleme durchnummerieren, so dass schon die für Mathematik, Physik und Ingenieurwissenschaften so wichtigen reellen Zahlen in Algorithmen nur approximativ bearbeitet werden können. So brauchen viele berechenbare Probleme so lange, dass man nicht auf die Ergebnisse warten kann, oder benötigen mehr Speicherplatz, als es Atome im Universum gibt. So lassen sich berechenbare Probleme formulieren, zu denen keine algorithmische Lösung bekannt ist. So kann man bei Programmen im Allgemeinen nicht wissen, was sie tun oder ob sie das Gewünschte tun. Für ein KI-System bedeutet das, dass es vielleicht „intelligent“ ist, man kann es aber nicht zeigen, oder es braucht mehr Zeit oder Speicherplatz als verfügbar ist. Andersherum könnte Intelligenz berechenbar sein, aber es lässt sich kein Algorithmus dafür finden. Interessanterweise kümmern sich die meisten Entwicklerinnen und Entwickler von KI-Systemen wie die von informationsverarbeitenden Systemen allgemein wenig um diese grundsätzlichen Grenzen, sondern begnügen sich mit dem Machbaren.

Andererseits folgt aus der Turingschen These auch, dass alles Regelhafte eine gute Chance hat, berechen- und programmierbar zu sein. So gesehen sind die Erfolge der KI bei diversen Spielen, bei Sprach- und Bildverarbeitung und bei Robotersteuerung nicht gar so überraschend, weil sie Regeln folgen, wenn auch sehr komplizierten. Sehr bedenklich sind dann allerdings Anwendungsversuche, für die keine Regeln bekannt sind und denen eventuell gar keine programmierbaren Regeln innewohnen wie politische Krisen und Kriege.

2.3 Das Unvergleichliche vergleichen

Wenn es stimmt, dass natürliche Intelligenz in ihren Wirkprinzipien weitgehend unbekannt und unverstanden ist, kann ein Vergleich mit KI nur auf der phänomenologischen Ebene erfolgen. Da ist zu konstatieren, dass die technischen Hervorbringungen der KI in vielen Einzelfällen den entsprechenden menschlichen Aktivitäten insbesondere bei Geschwindigkeit und Arbeitsumfang überlegen sind.

Wenn die Charakterisierungen von natürlicher und künstlicher Intelligenz in den vorigen beiden Unterabschnitten zutreffen, sind beide doch sehr verschieden voneinander. KI-Systeme sind von Menschen entwickelt und führen aus, was ihre Programme festlegen – ohne jeden eigenen Ehrgeiz. Was sie leisten, sind engbegrenzte Spezialleistungen. Jeder Mensch – auch schon ein kleines Kind – dagegen verfügt über eine Fülle intelligenter Fähigkeiten. Sie sind genetisch bedingt, werden vom Gehirn gesteuert und hängen in ihrer Ausprägung auch von Lebensumständen ab. Aber wie sie zustande kommen, ist offen.

Nach der Turingschen These gibt es drei Möglichkeiten, wie sich natürliche und künstliche Intelligenz zueinander verhalten können:

1. Natürliche Intelligenz ist berechenbar im Sinne der Turing-Berechenbarkeit. Dann ist sie programmierbar mit den heutigen Programmiersprachen und den heutigen Computern. Bisher scheint es aber keine erfolgversprechenden Ansätze dafür zu geben.

2. Sie ist berechenbar, aber jenseits der Turing-Berechenbarkeit und widerlegt damit die Turingsche These. Das wäre eine Nobelpreis-verdächtige Sensation, aber nichts deutet bisher darauf hin, dass sich das zeigen lässt.

3. Sie ist etwas ganz anderes.

Trotz aller Fortschritte in Biologie, Medizin, Psychologie, Kognitionswissenschaft und Hirnforschung ist unbekannt, welche Möglichkeit zutrifft. Ein interessanter Aspekt in dem Zusammenhang ist die Sicht der Philosophie in ihren vielen Verästelungen. Die Intelligenz wird da wenig direkt betrachtet und diskutiert, dagegen geht es eher um Vernunft, Geist und Seele. Das ändert aber wenig an der grundsätzlichen Frage, nur müsste man dann auf der technischen Ebene von Künstlicher Vernunft, Künstlichem Geist und von Künstlicher Seele sprechen.

3 KI zwischen Heilsbotschaft und Albtraum – Statt eines Fazits

Künstliche Intelligenz und Robotik ordnen sich bezogen auf den heutigen Entwicklungsstand voll und ganz in den allmählichen Prozess der Digitalisierung und Algorithmisierung der letzten Jahrzehnte ein. Damit sind neue Möglichkeiten verbunden, sie unterscheiden sich aber methodisch und technisch nur marginal von anderen informations- und kommunikationstechnischen Bereichen.

Was die allgemeine KI betrifft, so gab und gibt es eine Reihe von Versuchen, Systeme zu entwickeln, die intelligent sind und das nicht nur nachahmen, die aber anscheinend bisher nicht von Erfolg gekrönt sind. Die allgemeine KI bewegt sich – freundlich ausgedrückt – im Reich der Spekulation. Weniger freundlich könnte man sagen, dass es sich um Irreführung handelt. Wenn beispielsweise behauptet wird, den Systemen fehle lediglich Selbstbewusstsein, dann wird dabei übersehen, dass sowohl

völlig unklar ist, wie Selbstbewusstsein programmiert werden könnte, als auch dass den heutigen KI-Systemen noch viel mehr fehlt wie z. B. Witz, Ehrgeiz, Einfühlungsvermögen, Phantasie, Zweifel, Verantwortungsbewusstsein usw. Leider sind auch die eigentlich seriös arbeitenden Fachleute der schwachen KI gegenüber der Öffentlichkeit (und der Politik) nicht immer ganz ehrlich, wenn sie sich zur Intelligenz von KI-Systemen, zur Lernfähigkeit von lernenden Systemen und zur Autonomie autonomer Vehikel äußern.

Mit dem erreichten Stand der KI sind auch übertriebene Erwartungen, übersteigerte Hoffnungen und höchst problematische Anwendungsmöglichkeiten verbunden. KI wird von Politik und Wirtschaft weltweit als Schlüsseltechnologie gesehen, von der die zukünftige Wertschöpfung abhängt und die einen signifikanten Teil der heutigen Arbeitsplätze obsolet werden lassen könnte. Die sich abzeichnenden Anwendungen im militärischen Kontext führen zu einer gigantischen Rüstungsspirale, was die Gefahr von Kriegen wohl kaum verringern wird. KI-basierte Überwachungsmethoden lassen tiefe Eingriffe in die Privatsphäre und andere Grundrechte befürchten bis hin zu einer sozialen Totalüberwachung, wie sie in China auf der Tagesordnung steht. Selbst Allmachts- und Weltbeherrschungsphantasien gründen sich auf eine angestrebte Führungsrolle in der KI. Einige KI-Vertreter gehen noch viel weiter und propagieren die Entwicklung einer Superintelligenz, die nicht nur ähnliche Leistungen erbringt wie menschliche Intelligenz, sondern diese sogar in Gänze übertrifft. Wenn da etwas dran wäre, könnte das in ein Horrorszenario führen.

Ob die Blütenträume in Wirtschaft und Politik reifen, muss sich noch erweisen. Die gigantischen staatlichen und privatwirtschaftlichen Investitionen werden nicht völlig wirkungslos bleiben. Aber ob wissenschaftliche Durchbrüche und technologische Innovationssprünge gelingen, die auch kommerziell erfolgreiche Anwendungen nach sich ziehen, ist nicht garantiert. Nach der ersten KI-Euphorie im Laufe der zweiten Hälfte des 20. Jahrhunderts gab es eine Phase der Ernüchterung, die als KI-Winter bezeichnet wird und in der die KI Mühe hatte, Fördermittel zu akquirieren. Es ist nicht ausgeschlossen, dass auf den jetzigen KI-Sommer wieder ein KI-Winter folgt.

Es ist also dringend geboten, das Mögliche und Wünschenswerte vom Märchenhaften, Phantastischen und Schrecken Einflößenden zu trennen und die weitere Entwicklung kritisch zu begleiten. Viele Aspekte rund um die KI sind in dem Artikel nur angerissen. Eine vertiefende Diskussion von einigen davon kann man in der Dokumentation der FIfF-Konferenz 2019 mit dem Motto Künstliche Intelligenz als Wunderland finden, die in der *FIfF-Kommunikation* 1/2020 abgedruckt ist (Ahlmann et al. 2020).

Referenzen

Michael Ahlmann, Hans-Jörg Kreowski, Philip Love, Ralf E. Streibl, Karin Vosseberg, Margita Zallmann Hg. (2020) Künstliche Intelligenz als Wunderland. FIfF-Kommunikation 1/2020, 14-58.

Die Bundesregierung (2018) Strategie Künstliche Intelligenz der Bundesregierung. November 2018, https://www.bmbf.de/files/Nationale_KI-Strategie.pdf, abgerufen am 14.11.2020.

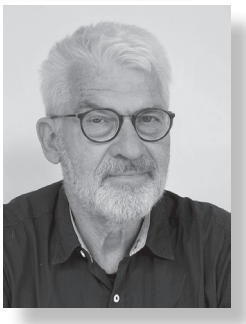
Epoch Times (2017) Putin zur künstlichen Intelligenz: „Wer in KI-Technologien führt, beherrscht die Welt", in: https://www.epochtimes.de/politik/ausland/putin-zur-kuenstlichen-intelligenz-wer-in-ki-technologien-fuehrt-beherrscht-die-welt-a2210862.html, abgerufen am 1.12.2020.

Dietmar Harhoff, Stefan Heumann, Nicola Jentzsch, Philippe Lorenz (2018) Eckpunkte einer nationalen Strategie für Künstliche Intelligenz. Stiftung neue Verantwortung, Berlin 2018, https://www.stiftung-nv.de/sites/default/files/ki_strategie.pdf, abgerufen am 14.11.2020.

Felix Hasler (2012) Neuromythologie – Eine Streitschrift gegen die Deutungsmacht der Hirnforschung. transscript Verlag, Bielefeld 2012.

John McCarthy, Marvin L. Minsky, Nathaniel Rochester, Claude E. Shannon (1955) A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence, http://www-formal.stanford.edu/jmc/history/dartmouth/dartmouth.html, abgerufen am 1.12.2020.

Alan M. Turing (1937) On Computable Numbers, with an Application to the Entscheidungsproblem. In: Proceedings of the London Mathematical Society, 2 (42), 230-265.



Hans-Jörg Kreowski und Wolfgang Krieger

Hans-Jörg Kreowski (Jahrgang 1949) ist Professor (i. R.) für Theoretische Informatik an der Universität Bremen. Er ist Mitglied im Vorstand des Forums InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF) und vertritt das FIfF im Vorstand der Zeitschrift Wissenschaft und Frieden. Er ist Mitglied der Leibniz-Sozietät der Wissenschaften zu Berlin, wo er zusammen mit Wolfgang Hofkirchner in Wien den Arbeitskreis Emergente Systeme, Information und Gesellschaft organisiert. Seit 2019 ist er außerdem Mitherausgeber des Grundrechte-Reports.

Wolfgang Krieger (Jahrgang 1946) ist Doktorand in der Arbeitsgruppe von Professor Kreowski. Er ist Diplom-Mathematiker (Algebraische Systemtheorie) und Ingenieur (FH, Regelungstechnik). Einen großen Teil seines bisherigen Berufslebens hat er sich mit dem Entwurf und der Realisierung von Expertensystemen und der Künstlichen Intelligenz beschäftigt. Er war u. a. Projektleiter und Mitautor des modellbasierten Diagnosesystems ROSE (Reasoning Over Systems in their Entirety).

Anja Gerlmaier

Gesund arbeiten im Home-Office: Was lehrt uns die Corona-Krise?

Seit das Infektionsschutzgesetz im März 2020 in Kraft trat, ist die Arbeitswelt vieler Erwerbstätiger aus den Fugen geraten: durch Betriebsschließungen etwa im stationären Einzelhandel, in der Gastronomie oder im Veranstaltungsmanagement brachen existenzielle Grundlagen ein, gingen Beschäftigte aufgrund von Auftragseinbußen in Kurzarbeit. Und wer nicht zwingend in den Betrieb musste, der sollte nach dem Willen des Gesetzgebers seine Arbeit besser im Home-Office durchführen. Im ersten Lockdown 2020 kam dieser Forderung schätzungsweise jeder vierte Erwerbstätige in Deutschland nach. Stellt das Home-Office à la Corona ein erstrebenswertes Zukunftsmodell flexibler Arbeit dar? Und was müssten Betriebe tun, damit es nicht zur Stress- oder Karriere-Falle mutiert? Der Beitrag beleuchtet zunächst die Entwicklung der Home-Office-Nutzung vor und während der Krise. Dem schließen sich arbeitswissenschaftliche Erkenntnisse zu Risiken oder Potenzialen dieser Form mobilen Arbeitens an. Der Beitrag schließt mit Gestaltungsempfehlungen für betriebliche Gestaltungs-Akteure und Beschäftigte, die bereits im Home-Office arbeiten oder dies planen.

Home-Office vor und in der Krise

In Deutschland fristete das Home-Office, also die überwiegende oder teilweise Arbeit von zu Hause aus, im Vergleich zu anderen EU-Ländern lange Zeit ein Schattendasein: Im Jahr 2016 arbeiteten beispielsweise lediglich 8 % der Arbeitnehmer:innen so (Schröder, 2020; Kohlrausch und Zucco, 2020). Home-Office stellte oft ein Privileg insbesondere für hochqualifizierte Spezialisten oder Führungskräfte dar oder war in vielen Betrieben nur einem engen Kreis von Beschäftigten, meist mit Sorgeverantwortung, gewährt worden (Grunau et al., 2019). Unternehmensvertreter:innen begründeten fehlende Home-Office-Konzepte oft mit zusätzlichen Kosten für die technische Ausstattung oder Datenschutzbedenken (Bonin et al., 2020). Das Inkrafttreten des Infektionsschutzgesetzes im März 2020 führte allerdings relativ schnell zu einem regelrechten Gesinnungswandel in vielen Betrieben, denn nun war es möglich, in kürzester Zeit für Tausende Beschäftigte technische Voraussetzungen zu mobilem Arbeiten zu schaffen (zum Begriff siehe auch Kasten auf der nächsten Seite). Dieser Digitalisierungsschub führte dazu, dass laut einer repräsentativen Erwerbstätigen-Befragung der Hans-Böckler-Stiftung zu Beginn der Corona-Krise im April 2020 27 % aller Erwerbstätigen überwiegend im Home-Office arbeiteten (Emmler/Kohlrausch, 2021). Der größte Teil davon (74 %) war mit neuen Formen flexibler Arbeit durchaus zufrieden, trotz zum Teil erheblicher widriger Umstände wie technischer und familiärer Betreuungsprobleme (Ernst, 2020). Die Zahl der überwiegend im Home-Office Tätigen sank Im Verlauf des Sommers vermutlich aufgrund geringerer Inzidenzzahlen auf 16 %. Trotz steigender Corona-Inzidenzen erhöhte sich der Anteil dauerhaft im Home-Office Tätiger im 2. Lockdown im November 2020 nicht (14 %). Dieser Umstand führte dazu, dass die Bundesregierung Ende Januar 2021 in einer neuen Arbeitsschutzverordnung Arbeitgeber dazu verpflichtete, Home-Office anzubieten, wenn keine zwingenden betrieblichen Gründe dagegensprechen (vgl. BMAS 2021).

Wie in Abbildung 1 dargestellt, erhöhte sich im Anschluss an diese Maßnahme der Anteil derjenigen, die ihre Arbeit schwerpunktmäßig aus dem Home-Office verrichteten, ungefähr auf das Niveau aus dem April 2020 (24 %) (Emmler/Kohlrausch, 2021).

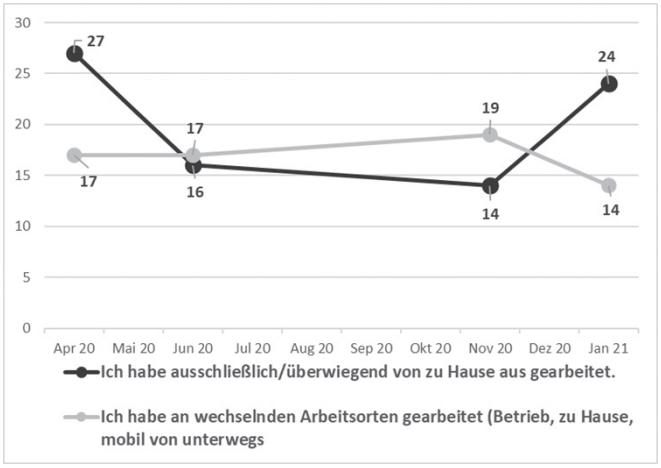


Abbildung 1: Nutzung von Home-Office und mobiler Arbeit seit 2020. Quelle: Emmler/Kohlrausch, 2021

Wie geht es weiter mit dem Home-Office, wenn der Infektionsschutz als Begründung wegfällt?

Nach einer Studie des BIBB/IAB will mehr als jeder zweite Betrieb nach der Krise wieder zum vorherigen Präsenzbetrieb zurückkehren (Bellmann et al., 2020). Nur jedes fünfte Unternehmen plant eine Ausweitung von Home-Office, jeder zehnte Betrieb möchte bestehende Regelungen sogar zurückfahren. Im Kon-

Anja Gerlmaier

Dr. phil. **Anja Gerlmaier** ist Arbeitspsychologin, Projektleiterin und wissenschaftliche Mitarbeiterin am Institut Arbeit und Qualifikation der Universität Duisburg-Essen, Abteilung Arbeitszeit und Arbeitsorganisation. Arbeitsschwerpunkte: Stressprävention, betriebliches Gesundheitsmanagement/Gefährdungsbeurteilung, betriebliche Konsequenzen des demografischen Wandels/lebensphasenorientierte Personalpolitik, betriebliche Digitalisierungsprozesse und Gestaltungskompetenz.
E-Mail: *anja.gerlmaier@uni-due.de*

Home-Office, Telearbeit, Mobile Arbeit – eine Begriffsbestimmung

Home-Office

Arbeitsform, bei der außerhalb der Betriebsstätte und von privaten Räumen des Arbeitnehmers aus gearbeitet wird. Unterscheidung zwischen zwei Formen:

Telearbeit

Nach § 2 Absatz 7 der Arbeitsstättenverordnung vom Arbeitgeber fest eingerichtete Bildschirmarbeitsplätze im Privatbereich der Beschäftigten. Arbeitgeber und Beschäftigte legen die Bedingungen der Telearbeit arbeitsvertraglich oder im Rahmen einer Vereinbarung fest. Der Arbeitgeber kommt für die benötigte Ausstattung des Telearbeitsplatzes mit Mobiliar, Arbeitsmitteln sowie Kommunikationseinrichtungen auf.

Mobile Arbeit

Arbeiten außerhalb von Betriebsstätten, was die Arbeit von zuhause aus wie von unterwegs oder vor Ort bei Kunden umfassen kann. Meist stellt der Arbeitgeber hierfür Notebooks und Smartphones für die Tätigkeitsausführung zur Verfügung.
Mobiles Arbeiten ist im Gegensatz zu Telearbeit nicht gesetzlich geregelt. Es besteht aber die Möglichkeit, Betriebs- oder Dienstvereinbarungen zwischen dem Arbeitgeber und der Interessenvertretung zur mobilen Arbeit abzuschließen.

Unabhängig von der Form des häuslichen Arbeitens (Telearbeit oder mobile Arbeit) ist der Arbeitgeber nach §§ 3 und 5 ArbSchG dazu verpflichtet, die mit der ortsflexiblen Arbeit verbundenen Gesundheitsgefährdungen zu ermitteln (Gefährdungsbeurteilung) und gemäß der gesetzlichen Präventionsanforderungen zu beseitigen oder zumindest zu minimieren.

trast dazu wünschen sich nach einer Studie der Krankenkasse DAK 77 % erstmals im Home-Office arbeitender Beschäftigter, das Arbeiten von zu Hause aus weiter fortführen zu können (DAK Gesundheit, 2020).

In so manchem Betrieb sind infolgedessen in Sachen Home-Office neue Konfliktfelder programmiert. Sie schließen an eine seit Jahren zwischen Arbeitgebern und Gewerkschaften geführte Kontroverse an, wie viel Home-Office gut für Unternehmen oder Arbeitnehmer sein könnte, und wie viel Regulierungsbedarf hier sinnvoll ist.

Die Licht- und Schattenseiten des Home-Office

Aktuell vergeht kaum eine Woche, in der nicht neue Erkenntnisse zum Pro und Kontra durch die Medien gehen. Lässt man wie in einer Studie der DAK aus dem Mai 2020 (DAK Gesundheit, 2020) die betroffenen Beschäftigten zu Wort kommen, so sehen viele trotz der Krisensituation mit der Ausgestaltung ihres Arbeitsplatzes zu Hause positive Veränderungen ihrer Arbeits- und Lebenssituation:

- 68 % schätzten den Zeitgewinn durch die wegfallenden Fahrzeiten als positiv ein.
- 65 % bewerteten es als positiv, die Arbeit besser über den Tag verteilen zu können.
- 57 % fanden, dass der Arbeitsdruck im Home-Office geringer ist als im Büro.

Diesen Vorteilen stellten die befragten Beschäftigten aber auch etliche Nachteile gegenüber. Bemängelt wurden vor allem der verringerte direkte Kontakt zu den Kollegen (75 %) und die Möglichkeit, sich kurzfristig – auch mit dem Chef – zu besprechen (48 %). Jeder zweite Befragte empfand es darüber hinaus als unangenehm, dass eine klare Trennung von Berufs- und Privatleben im Home-Office schwierig war. Neben Problemen der Informationsweitergabe und kollegialen Unterstützung gerät das Home-Office aktuell auch immer mehr als möglicher gesundheitlicher Risikofaktor in den Fokus des öffentlichen Interesses: Nach einer Studie der DEKRA klagte jeder dritte Beschäftigte im Home-Office über Verspannungen, Rückenschmerzen und Kopfschmerzen (DEKRA, 2021). Der Bericht kommt deshalb zu dem Schluss, dass Home-Office krank machen würde. Unterbelichtet bleibt bei vielen dieser derzeit kursierenden Corona-Studien allerdings, ob die gesundheitlichen Beschwerden tatsächlich durch das Arbeiten im Home-Office oder andere Faktoren verursacht sind. Betrachtet man Studien mit Vergleichsgruppen wie etwa von der AOK aus dem Jahr 2019, so zeigt sich nämlich, dass Beschäftigte im Büro, im Home-Office oder bei Mobilarbeit mit ca. 40 % ein vergleichbares Ausmaß an Kopfschmerzen verspüren (Waltersbacher et al., 2019, vergleiche auch Abbildung 2).

Wer sich bei den zahlreichen Corona-Studien zum Thema Home-Office auf die Suche nach wissenschaftlich fundierten Analysen zu Ursachen etwa von gesundheitlichen Beschwerden und Stress bei der Arbeit im Home-Office macht, der wird aktuell enttäuscht. Glücklicherweise gibt es aus der Vor-Corona-Zeit eine ganze Reihe arbeitswissenschaftlich gut fundierte Studien, die uns Hinweise über Gesundheitspotenziale und Risiken bei der Arbeit im Home-Office als Basis für eine humanzentrierte

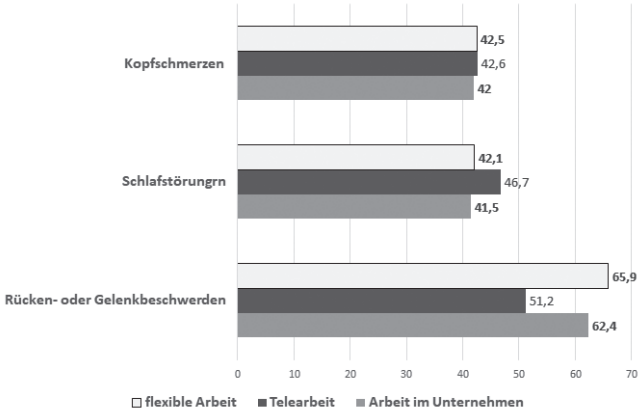


Abbildung 2: Beeinträchtigungen und gesundheitliche Beschwerden (Angaben in Prozent (Nennung „ständig" und „häufig", 5-stufige Skala), Quelle: Waltersbacher et al. 2019. (bundesweite telefonische Befragung der Ortskrankenkassen, n=2001))

Hinweis zu Abbildung 2: Arbeit im Unternehmen = 100 % der Arbeitszeit im Unternehmen, Telearbeit = überwiegender Teil der außerbetrieblichen Arbeitszeit von zu Hause, flexible Arbeit = überwiegender Teil der außerbetrieblichen Arbeitszeit nicht von zu Hause

Arbeitsgestaltung geben können. Hier ergibt sich folgendes Bild:

- Im Home-Office Arbeitende weisen deutlich weniger Fehlzeiten und eine höhere Produktivität auf, wenn sie abwechselnd zu Hause und im Büro und auf freiwilliger Basis im Home-Office arbeiten können (Lynch, 2017).

- Die Arbeit im Home-Office kann die Konzentrationsfähigkeit verbessern und das Burnout-Risiko vermindern, wenn Beschäftigte hierdurch weniger Störungen und einem geringeren Geräuschpegel (zum Beispiel in Großraumbüros) ausgesetzt sind (Andriessen und Roe, 1994; Gerlmaier, 2019).

- Beschäftigte im Home-Office sind zufriedener mit ihrer Arbeit als Kollegen im Büro, wenn sie im Home-Office zeitungebundener arbeiten können als im Büro (Schmook und Bendrien, 2004). Dies gilt insbesondere, wenn reduzierte Fahrzeiten konsequent zu Erholungszwecken genutzt werden (Lott, 2019).

Studien der Bundesanstalt für Arbeitsschutz und Arbeitsmedizin zeigen, dass bei der Arbeit im Home-Office oder mobiler Arbeit auch Gefährdungen für die psychische Gesundheit und unerwünschte Entgrenzungen von Arbeiten und Leben auftreten können. Diese sind jedoch häufiger in Arbeitskontexten zu beobachten, in denen es an betrieblichen Regelungen und Gestaltungs-Know-how mangelt (Backhaus/Wöhrmann/Tisch, 2019). Wurden in Betrieben Home-Office-Lösungen eingeführt, so standen dort häufig Fragen der ergonomischen Gestaltung des häuslichen Arbeitsplatzes im Vordergrund. Es liegt auf der Hand, dass ungeeignete Arbeitsumgebungen oder unergonomische Arbeitsmittel (Laptop-Tastaturen oder Displays) bei längerer Exposition zu Beschwerden wie Konzentrationsstörungen, Kopfschmerzen oder muskulo-skelettalen Beschwerden führen (Tegtmeier, 2016). Bei der Gestaltung von Tele- oder mobiler Arbeit deutlich weniger beachtet wurden dagegen die erheblichen gesundheitlichen Gefährdungspotenziale durch psychosoziale Belastungen:

- Unrealistische oder unklare Ergebniserwartungen führen im Home-Office häufiger zu überlangen Arbeitszeiten, einer selbst organisierten Verkürzung von Pausen oder zu erweiterten Erreichbarkeitsangeboten. Diese können zu psychischer Erschöpfung, Schlafproblemen und familiären Konflikten beitragen (zusammenfassend Rau/Göllner, 2019).

- Häufige Abwesenheit vom Betrieb in Kombination mit unzureichenden Kommunikationsroutinen begünstigen das Risiko für soziale Isolierung und eingeschränkte Karriere- und Weiterbildungschancen aufgrund geringerer *Sichtbarkeit* für Vorgesetzte und Kollegen (Koehne et al. 2012).

Mit der durch die Pandemie weiter beschleunigten Digitalisierung treten im Home-Office additiv neuartige kognitive Beanspruchungsrisiken auf, beispielsweise die sogenannte „Zoom-Müdigkeit" (Rump/Brandt, 2020). Beschrieben wird hiermit Müdigkeit, die während oder nach zahlreichen virtuellen Meetings am Tag und in der Woche verspürt wird und die offenbar das Risiko von Konzentrationsstörungen, Gereiztheit, Kopf- und Rückenschmerzen deutlich erhöht.

Die Studienlage zeigt auch, dass sich Stressrisiken ungleich verteilen und sich bei Müttern zu kumulieren scheinen: Mütter im Home-Office arbeiteten auch schon vor der Pandemie im Durchschnitt drei Stunden länger als im Büro tätige Kolleginnen (Lott, 2019), im Vergleich zu Vätern sind sie häufiger parallel zu ihrer Tätigkeit mit der Beaufsichtigung ihrer Kinder und Haushaltsaufgaben beschäftigt, was mit einer höheren Unzufriedenheit und offenbar auch mit einem höheren Burnout-Risiko einhergeht. Nach einer aktuellen Studie der Bertelsmann Stiftung gaben 49 % der im Home-Office arbeitenden Mütter an, dass während des Lockdowns ihre psychischen, emotionalen oder körperlichen Puffer erschöpft seien. Bei den Vätern waren es 31 % (von Würzen, 2020).

Home-Office gesund und produktiv gestalten: Was sollte bei der Planung und Umsetzung beachtet werden?

Die Corona-Krise offenbart in zunehmend mehr Betrieben, dass neue Formen ortsflexibler Arbeit, wozu auch die Arbeit zu Hause zählt, schnell zu Frust und Stress führen, wenn sie nicht intelligent geregelt und fair gestaltet werden. Arbeitsschutz-Akteure, Führungskräfte und Beschäftigte tun gut daran, die in der Pandemie gewonnenen Erkenntnisse über die Licht- und Schattenseiten des Home-Office sinnvoll zu nutzen und intelligente Gestaltungslösungen kollektiv anzugehen. Unternehmen sind im Rahmen von §§ 3 und 5 ArbSchG ohnehin dazu verpflichtet, die mit der ortsflexiblen Arbeit verbundenen Gesundheitsgefährdungen zu ermitteln (Gefährdungsbeurteilung) und gemäß der gesetzlichen Präventionsanforderungen zu beseitigen oder zumindest zu minimieren. Bedarfsgerechte, fair ausgehandelte Regeln, zum Beispiel im Rahmen von Betriebsvereinbarungen, auf Basis solcher Gefährdungsbeurteilungen können helfen, Orientierung zu geben und wechselseitiges Vertrauen aufzubauen.

Was sollte beachtet werden, wenn Vereinbarungen zum Home-Office oder zur mobilen Arbeit auf der Agenda eines Unternehmens stehen?

Folgende Leitlinien können helfen, das Arbeiten ressourcenstärkend zu gestalten:

- Freiwilligkeit als Maxime betrieblicher Gestaltung: Mobile oder Arbeit vom häuslichen Arbeitsplatz aus sollte auf freiwilliger Basis geschehen und den Arbeitnehmern die Möglichkeit geben, auch an einem Arbeitsplatz in der Betriebsstätte arbeiten zu können.

- Alternierende Home-Office Lösungen bevorzugen: Der Wechsel zwischen der Arbeit zu Hause und im Büro eröffnet mehr Kooperationsmöglichkeiten und Chancen zum Aufbau und Erhalt von sozialen Beziehungen im Betrieb. Risiken der Arbeit im Home-Office, zum Beispiel Bewegungsmangel, Isolierung und Entgrenzungsprobleme lassen sich hierdurch verringern (Treier, 2003).

- Arbeitsplatzergonomie: Bei regelmäßiger Arbeit von zu Hause ist die Einrichtung eines ergonomischen Arbeitsplatzes nach Arbeitsstättenverordnung (Telearbeit) empfehlenswert (Lafrenz & Wirth, 2019).

- Arbeitszeit und Pausenregelungen: Betriebliche Regelungen zu Anwesenheits- und Abwesenheitszeiten oder zu Reaktionszeiten auf E-Mails oder andere Kontaktanfragen haben sich bewährt, damit Beschäftigte weniger Stress im Home-Office empfinden und zeitliche Freiheitsgrade überhaupt nutzen können (Backhaus/Brauner/Tisch, 2019).

- Arbeitszeitdokumentation: Wie im Büro auch sollten Arbeitszeiten im Home-Office dokumentiert und die Möglichkeit zum Freizeitausgleich geregelt werden.

- Information und Kommunikation: Probleme beim Informationsaustausch oder bei der kollegialen Unterstützung können durch feste Anwesenheitszeiten in der Betriebsstätte gelöst werden. Die Einrichtung regelmäßig stattfindender Teamsitzungen mit Anwesenheitspflichten für das gesamte Team kann den Informationsaustausch und die sozialen Beziehungen mit Kollegen und Vorgesetzten stärken (Backhaus/Brauner/Tisch, 2019)

- Schaffung von virtuellen Räumen im Betrieb zum informellen Austausch unter Kollegen (zum Beispiel Betriebs-Chatrooms oder Räume für virtuelles Kaffeetrinken): Sie können den informellen Informationsaustausch unter Kollegen fördern. Hilfreich ist es, wenn sie in regelmäßigen Abständen stattfinden, Transparenz über die Teilnehmer existiert und freiwillige Moderatoren für dieses Kommunikationsformat gefunden werden.

- Kommunikationskulturen partizipativ gestalten: Regeln zu Kommunikation und Arbeitszeiten sind nur dann wirklich wirksam, wenn entsprechende Kulturen hierzu entwickelt werden (Gerlmaier, 2020). Führungskräfte sind gefragt, mit ihren Teams bedarfsangepasste Regeln zu erarbeiten und transparent zu machen (zum Beispiel Dokumentation im Intranet, Team-Wiki).

- Arbeitsintensität besprechbar machen: Für Phänomene wie hohe Arbeitsintensitäten, das Durcharbeiten ohne Pausen und überlange Arbeitszeiten ist selten der Heimarbeitsplatz ursächlich. Die Wurzeln liegen oft in unrealistischen und überzogenen Ergebniserwartungen von Führungskräften oder Auftraggebern begründet und fördern wiederum verausgabendes Leistungsverhalten (vgl. Krause et al., 2015). Eine Verlagerung der individuellen Arbeitsplanung und Rückkopplung der erarbeiteten Ergebnisse auf die Teamebene (zum Beispiel in Team-Meetings mit der Führungskraft) können individuellen Überforderungsrisiken im Home-Office durch kollektive Achtsamkeit vorbeugen.

- Qualifizierung: Beschäftigte und Führungskräfte müssen durch Qualifizierungsmaßnahmen und Unterweisungen unbedingt auf das Arbeiten in Distanz vorbereitet werden. Ansonsten droht Stress, weil etwa Kompetenzen zum Umgang mit Videokonferenzen oder anderem technischem Equipment unzureichend vorhanden sind oder nur geringe Gestaltungskompetenz im Umgang mit selbstorganisiertem Arbeiten existiert (Gerlmaier/Geiger 2019).

Gesund und entspannt bleiben im Home-Office: die individuelle Seite der Gestaltung

Damit die Arbeit im Home-Office produktiv und gleichzeitig gesundheitsstärkend vonstatten gehen kann, sind wie oben beschrieben angemessene technische Voraussetzungen und neue Formen der Arbeitsorganisation von Seiten des Betriebes notwendig. Eine ebenso bedeutsame Größe für den Erfolg stellen aber auch individuelle Einstellungen und Gestaltungskompetenzen dar. Was können wir also selbst tun, damit das Home-Office nicht zu einer Stressfalle wird? Folgende praktische Tipps sind:

- Bewusst Grenzen der Arbeit setzen. Dies kann durch eine räumliche Trennung (zum Beispiel Arbeitszimmer), das bewusste Setzen eines Arbeitsendes oder durch das Einplanen von Freizeitaktivitäten nach dem Arbeitsende geschehen.

- Planen und Durchführen regelmäßiger Kurzpausen (zum Beispiel alle 90 Minuten 5 bis 10 Minuten Pause). Die Pausen sind erholsamer, wenn der Arbeitsplatz verlassen und eine aktive Pausengestaltung vollzogen wird (zum Beispiel Bewegungsübungen oder einfach der Gang zum Postkasten).

- Geblockte Zeiten für konzentriertes Arbeiten (zum Beispiel 2 bis 2,5 Stunden) einplanen und durchsetzen. Ständige Störungen bei der Arbeit, etwa durch Familienangehörige oder Nachbarn und ein häufiger Wechsel von beruflichen und privaten Aufgaben mindern die Produktivität und das Selbstwirksamkeitserleben erheblich und sollten vermieden werden.

- Sind kleine Kinder oder pflegebedürftige Angehörige im Haus, sollten für diese alternative Betreuungspersonen während der Arbeitszeiten gesucht werden. Denkbar sind auch Wechselmodelle, bei denen Vater oder Mutter abwechselnd Betreuungszeiten übernehmen. Die Corona-Krise hat hier noch einmal eindrücklich gezeigt, dass der Versuch einer Bewältigung beider Rollenanforderungen ein erhebliches Burnout-Risiko birgt!

- Wenn Groupware oder andere Kollaborationssysteme genutzt werden, sollten frühzeitig Unterweisungen oder Qualifizierungen vom Arbeitgeber eingefordert werden, um die Digitaltechnik im Home-Office sicher zu beherrschen.

Fazit

Wird der durch die Pandemie beschleunigte Digitalisierungsschub auch in Post-Corona-Zeiten genutzt werden, um mehr Erwerbstätigen höhere Spielräume bei der Gestaltung ihrer Arbeits- und Lebenssphären zu ermöglichen? Oder wurde mit der Pandemie ein Zeitalter der vollständigen Entgrenzung eingeleitet, in der Selbstausbeutung, ständige Erreichbarkeit und virtuelle Kollegen das neue Normal für die noch in Beschäftigung befindlichen Arbeitenden darstellen? Wir alle tun gut daran, Stress im Home-Office nicht als Luxusproblem von Hochqualifizierten anzusehen, die es mit ein bisschen Selbstorganisationskompetenz schon zu richten wissen. Wenn das Home-Office zukünftig eine vom Infektionsschutz losgelöste, eigenständige Existenzberechtigung bekommen soll, sind kollektive und solidarische Gestaltungslösungen mehr denn je vonnöten. Die Schaffung notwendiger technischer Voraussetzungen bildet ebenso wie Gesetzesinitiativen für einen Anspruch auf Home-Office grundsätzlich gute Rahmenbedingungen. Damit Smart Work nicht eine Phrase auf politischen Positionspapieren bleibt, bedarf es vor allem aber beharrlicher Gestaltungs-Akteure innerhalb und außerhalb von Betrieben, denen angesichts der drohenden Wirtschaftskrise ein „Hauptsache Arbeit" nicht genug ist.

Literatur

Andriessen JH, Roe RA Eds. (1994) Telematics and Work. Sussex: Erlbaum

Backhaus N, Brauner C, Tisch A, (2019) Auswirkungen verkürzter Ruhezeiten auf Gesundheit und Work-Life-Balance bei Vollzeitbeschäftigten: Ergebnisse der BAuA-Arbeitszeitbefragung 2017. Z. Arb. Wiss.

Backhaus N, Wöhrmann AM, Tisch A (2019) BAuA-Arbeitszeitbefragung: Telearbeit in Deutschland (baua: Bericht kompakt). Dortmund/Berlin/Dresden: Bundesanstalt für Arbeitsschutz und Arbeitsmedizin. Abrufbar unter: ian, A.: Was bewegt Arbeitgeber in der Krise? Eine neue IAB Befragung gibt Aufschluss. In: IAB-Forum, https://www.iab-forum.de/was-bewegt-arbeitgeber-in-der-krise-eine-neue-iab-befragung-gibt-aufschluss/, zuletzt abgerufen: 11.5.2021

BMAS (Bundesministerium für Arbeit und Soziales) (2021) SARS-CoV-2-Arbeitsschutzverordnung (Corona-ArbSchV) vom 21. Januar 2021. Berlin: Bundesanzeiger. Abrufbar unter: BAnz AT 22.01.2021 V1.pdf (bundesanzeiger.de), zuletzt abgerufen: 11.05.2021

Bonin H, Eichhorst W, Kaczynska J, Kümmerling A, Rinne U, Scholten A, Steffes S (2020) Verbreitung und Auswirkungen von mobiler Arbeit und Homeoffice (Forschungsbericht Nr. 459). Berlin: Bundesministerium für Arbeit und Soziales.

DAK Gesundheit Hg. (2020) Gesundheitsreport 2020. IGES Institut GmbH. Hamburg. Internetdokumentaton: https://www.dak.de/dak/bundesthemen/gesundheitsreport-2020-2371690.html, zuletzt abgerufen: 11.5.2021

DEKRA (2021) Arbeitssicherheitsreport. Stuttgart: DEKRA

Emmler H, Kohlrausch B (2021) Homeoffice: Potenziale und Nutzung – Aktuelle Zahlen aus der HBS-Erwerbspersonenbefragung, Welle 1 bis 4. WSI Policy Brief Nr. 52. Düsseldorf: WSI

Ernst C (2020) Homeoffice im Kontext der Corona-Pandemie. Eine Ad-hoc-Studie der Technischen Hochschule Köln. Köln: TH

Gerlmaier A (2020) Gesundheitsressourcen stärken bei digitaler Produktionsarbeit: Evaluation des teambezogenen Stresspräventionskonzeptes "SePIAR". GfA, Dortmund (Hrsg.): Frühjahrskongress 2020, Berlin. Digitaler Wandel, digitale Arbeit, digitaler Mensch. Beitrag A.8.2

Gerlmaier A (2019) Blockzeiten für störungsfreies Arbeiten. In: Gerlmaier A, Latniak E Hg. (2019) Handbuch psycho-soziale Gestaltung digitaler Produktionsarbeit. Gesundheitsressourcen stärken durch organisationale Gestaltungskompetenz. Wiesbaden: Springer Gabler Verlag, S. 325-328

Gerlmaier A, Geiger L (2019) Arbeitsgestaltungskompetenz in der betrieblichen Praxis: Über welches Gefahren- und Gestaltungswissen verfügen Arbeitsschutz-Akteure, Führungskräfte und Beschäftigte? In: Gerlmaier A, Latniak E Hg. (2019) Handbuch psycho-soziale Gestaltung digitaler Produktionsarbeit. Gesundheitsressourcen stärken durch organisationale Gestaltungskompetenz. Wiesbaden: Springer Gabler Verlag, S. 79-92

Grunau P, Ruf K, Steffes S, Wolter S (2019) Mobile Arbeitsformen aus Sicht von Betrieben und Beschäftigten: Home-Office bietet Vorteile, hat aber auch Tücken. (IAB-Kurzbericht, 11/2019) Internetdokumentaton: http://doku.iab.de/kurzber/2019/kb1119.pdf, zuletzt abgerufen: 11.05.2021.

Koehne B, Shih PC, Olson JS (2012) Remote and Alone: Coping with Being the Remote Member on the Team. In: Poltrock S, Simone C, Grudin J, Mark G, Riedl J Eds. (2012), Proceedings of the ACM 2012 conference on Computer Supported Cooperative Work – CSCW'12 (p. 1257). New York: ACM Press

Krause A, Baeriswyl S, Berset M, Deci N, Dettmers J, Dorsemagen C, Meier W, Schraner S, Stetter B, Straub L (2015) Selbstgefährdung als Indikator für Mängel bei der Gestaltung mobil-flexibler Arbeit. Wirtschaftspsychologie Heft 4-2014/1-2015, 49-59.

Lafrenz B, Wirth M (2019) Moderne Büroraumgestaltung. In: Gerlmaier A, Latniak E Hg. (2019) Handbuch psycho-soziale Gestaltung digitaler Produktionsarbeit. Gesundheitsressourcen stärken durch organisationale Gestaltungskompetenz. Wiesbaden: Springer Gabler Verlag

Lott Y (2019) Weniger Arbeit, mehr Freizeit. WSI-Report 47. Düsseldorf: WSI

Lynch S (2017) Why Working from Home Is a "Future-Looking Technology". A Stanford GSB expert shows how companies and employees benefit from workplace flexibility. Abrufbar unter: https://www.gsb.stanford.edu/insights/why-working-home-future-looking-technology, zuletzt abgerufen: 11.05.2021.

Rau R, Göllner M (2019) Erreichbarkeit gestalten, oder doch besser die Arbeit? Zeitschrift für Arbeits- und Organisationspsychologie. 63 (1). S. 1-14

Rump J, Brandt M (2020) Zoom-Fatigue. Ludwigshafen: IBE. Abrufbar: https://www.ibe-ludwigshafen.de/zoom_fatigue/, zuletzt abgerufen: 11.05.2021

Schmook R, Bendrien J (2004) Belastungen, Beanspruchungen und Gesundheitsförderung bei telekooperativer Arbeit. In: Hertel G, Konradt U Hg. (2004) Human Resource Management im Inter- und Intranet. Göttingen: Hogrefe. S. 187-203

Tegtmeier P (2016). Review zu physischer Beanspruchung bei der Nutzung von Smart Mobile Devices (baua: Bericht). Dortmund / Berlin / Dresden: Bundesanstalt für Arbeitsschutz und Arbeitsmedizin. Abrufbar unter: https://www.baua.de/DE/Angebote/Publikationen/Berichte/Gd88.html zuletzt abgerufen: 11.5.2021

Treier M (2003) Belastungs- und Beanspruchungsmomente bei der Teleheimarbeit. Zeitschrift für Arbeits- und Organisationspsychologie, 47, S. 24-35.

von Würzen B (2020) Rollen und Aufgabenverteilung bei Frauen und Männern in Corona-Zeiten. Gütersloh: Bertelsmann Stiftung.

Waltersbacher A., Maisuradze M., Schröder H. (2020): Arbeitszeit und Arbeitsort – (wie viel) Flexibilität ist gesund? Ergebnisse einer repräsentativen Befragung unter Erwerbstätigen zu mobiler Arbeit und gesundheitlichen Beschwerden. In: Badura B, Ducki A, Schröder H, Klose J, Meyer M (Hrsg.) (2019) Fehlzeiten-Report 2019 – Digitalisierung – gesundes Arbeiten ermöglichen. Kapitel 7. Berlin: Springer-Verlag. S. 77-110.

Stephan Wiefling

Usable Security und Privacy – eine Einführung

Vortrag auf der FIfF-Konferenz am 14. November 2020

Transkription: Kai Nothdurft. Überarbeitung: Eberhard Zehendner.

Vielen Dank für die Einleitung und Anmoderation. Ich bin Stephan Wiefling, wissenschaftlicher Mitarbeiter bei der Gruppe für Daten- und Anwendungssicherheit von der Hochschule Bonn-Rhein-Sieg, der Gruppe von Prof. Dr. Luigi Lo Iacono. Wir arbeiten täglich an Usable-Security-und-Privacy-Themen. Das gehört bei uns zum Tagesgeschäft und deswegen freue ich mich natürlich sehr über die Einladung vom FIfF, das Thema hier vorstellen zu dürfen.

Wir werden Euch und Ihnen näherbringen, was uns so fasziniert an diesem Thema und wie man das vielleicht später umsetzen kann, eine kleine Einführung in Usable Security und Privacy.

Aber ich gehe jetzt mal davon aus, dass wir vielleicht nicht auf dem gleichen Stand sind, was IT-Sicherheit angeht. Näher betrachtet schauen wir uns Datenschutz und Datensicherheit an und was wollen wir damit erreichen?

Wir wollen Schutzziele erreichen. Das ist das Ziel in der IT-Sicherheit. Wir wollen uns vor allem vor Angreiferinnen und Angreifern schützen. Das können Amateure sein, das können Profis sein, das können aber auch staatliche Akteure sein. Die wollen uns beispielsweise abhören und davor wollen wir uns dann schützen.

Die wichtigsten dieser Schutzziele sind in Abbildung 1 dargestellt: Das sind so Begriffe wie Zurechenbarkeit, Zugriffskontrolle, Vertraulichkeit, Integrität, Verbindlichkeit. Das sind ganz tolle Wörter, die stehen bestimmt auch im Duden drin, aber ich denke mal, für den einen oder anderen werden diese wahrscheinlich schwer zu verstehen sein.

Abbildung 1: Wichtige Schutzziele der IT-Sicherheit. © Stephan Wiefling/Peter Leo Gorski (Montage) 2020. Designed by Freepik

Deswegen gehen wir jetzt ein bisschen näher rein in die Themen, um diese Begriffe ein bisschen genauer zu erklären. Inklusive der Erklärung dieser schwierigen Wörter gehen wir auch auf Beispiele von Auswirkungen ein, die auch im realen Leben vorkommen können.

Vertraulichkeit

Wenn wir beispielsweise auf einem Cloudserver Daten über uns speichern, dann wollen wir natürlich auch sicherstellen, dass diese Daten dann nur für uns zugänglich sind. Die Praxis zeigt leider auch, dass durch Datenschutzverletzungen oder Hacks Datensätze abhandenkommen. Es zeigt leider eindeutig, wie schwierig Datenschutz und Datensicherheit in der Praxis ist.

In Abbildung 2 ist eine große Anzahl an Hacks dargestellt. Die Größe der Kreise gibt an, wie viele Datensätze von Nutzerinnen und Nutzern abhandengekommen sind. Das ist schon eine beeindruckende Grafik, weil ich denke, manche dieser Dienste, die da in der Grafik dargestellt sind, werden wir alle in gewisser Weise mal benutzt haben oder zumindest einige davon.

Das sind schon Milliarden an Datensätzen, die da abhandengekommen sind. Wir dürfen aber nicht vergessen: Mit jedem

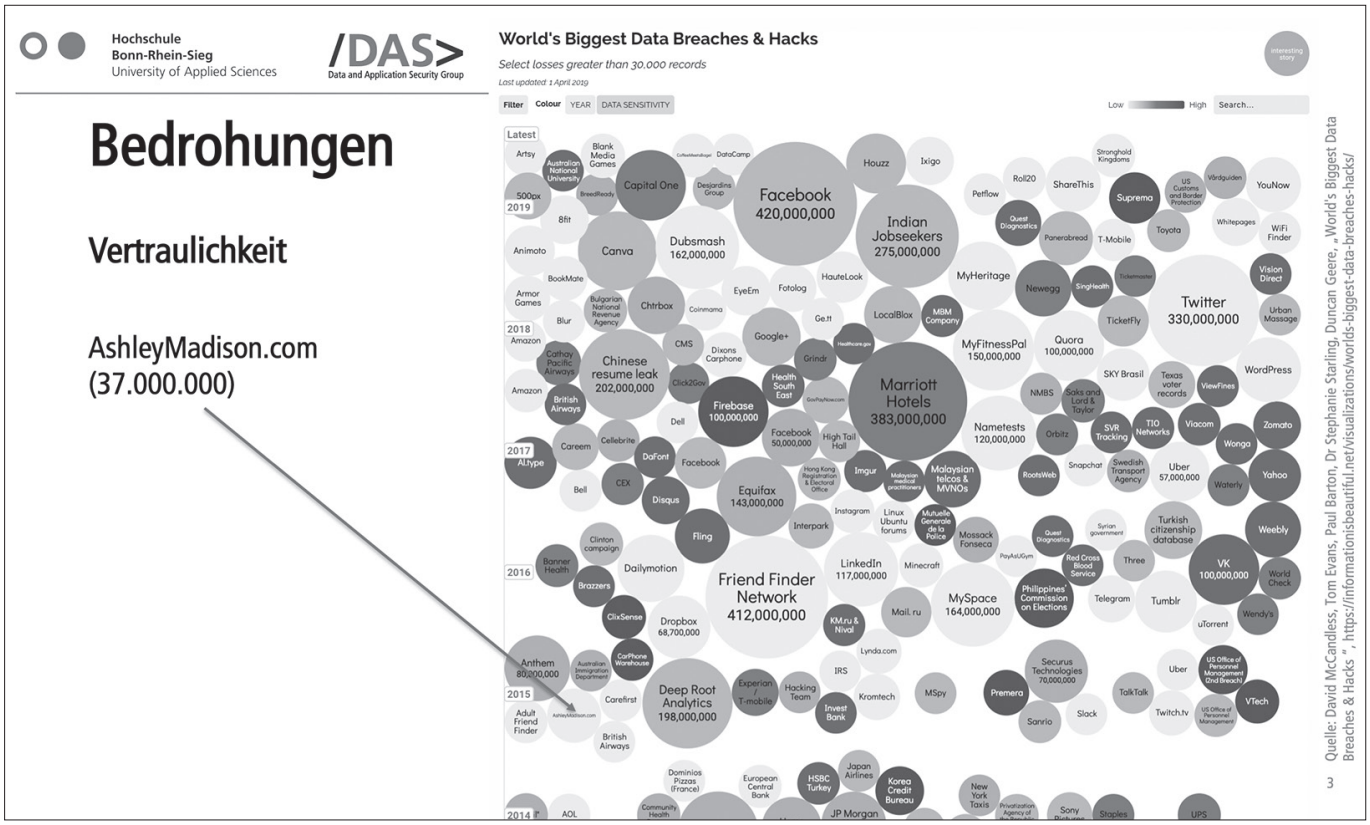


Abbildung 2: Reale Verletzungen von Vertraulichkeit.[1]
© Information is Beautiful 2019/Stephan Wiefling (Bearbeitung)/Peter Leo Gorski (Montage)

einzelnen abhandengekommenen Datensatz sind persönliche Schicksale und Konsequenzen verbunden. Wir nehmen mal als Beispiel die Webseite *Ashley Madison.*

Bei Ashley Madison können sich verheiratete Männer und Frauen anmelden, mit dem Ziel, eine Affäre zu suchen. Moralisch wollen wir nicht diskutieren über diese Webseite. Fakt ist aber, dass Datensätze der Kundinnen und Kunden komplett abhandengekommen sind. Wo persönliche Nachrichten dabei waren, Kreditkartendaten, Anschriften der Personen, die Namen, mit wem sie vermutlich eine Affäre aufgebaut haben, und Ähnliches. Und wenn der Datensatz einmal gestohlen wurde, dann haben wir keine Kontrolle mehr darüber. Die Folgen davon sind wirklich gravierend, denn wir hatten es in diesem Beispiel mit einem sehr gravierenden Eingriff in die Privatsphäre zu tun. Das ist dann wirklich kein Spaß mehr, denn, wenn ich jetzt diesen Datensatz habe, könnte ich mit diesem dann Leute erpressen, Identitätsdiebstahl, …

Im Fall Ashley Madison gab es sogar Fälle, die mit dem Tod geendet haben, das ist wirklich harter Stoff. Das wäre jetzt zum Beispiel eine echte Bedrohung mit Folgen, die wir in Bezug auf die Vertraulichkeit hätten.

Verbindlichkeit und Zurechenbarkeit

Bei dieser Webseite sind auch Kreditkartendaten geklaut worden. Es kommt leider in der Praxis sehr häufig vor, dass Online-Dienste unerlaubterweise auch den Sicherheitscode der Kreditkarte (CVC) speichern. Den Code darf man aber nicht speichern, weil damit eben jede Person valide Transaktionen mit meinem Geld durchführen kann. Wenn man sich also überlegt: *Angreifende* haben die Kreditkartennummer und die Sicherheitsnummer und wenn diese dann noch die Adresse dabeihaben, können sie in fremdem Namen einkaufen gehen.

Womit wir beim Punkt Verbindlichkeit und Zurechenbarkeit sind, denn jetzt kann jemand in meinem Namen Produkte bestellen. Das hat dann nicht nur strafrechtliche, sondern auch finanzielle Konsequenzen für mich und ich denke, wo wir jetzt eh alle in den COVID-19-Zeiten leben, da wird vermutlich der Kreditkartenbetrug noch mehr angestiegen sein oder zumindest auf hohem Niveau bleiben. Denn durch Social Distancing ist es vermutlich schwerer, den Geldbeutel zu klauen, weil wir ja in der Regel 1,5 m Abstand halten sollen und wenn sich da einer uns nähert, wirkt das verdächtig.

Integrität und Verfügbarkeit

Eine weitere Bedrohung ist die Integrität, also: *Wie erkenne ich, dass Daten von anderen manipuliert werden?* Das kann beispielsweise eine E-Mail sein. Ich bekomme vielleicht eine E-Mail von meinem Chef oder meiner Chefin mit dem Inhalt: „Sie sind gefeuert." Dann will ich natürlich wissen, ob die Mail wirklich von der entsprechenden Person versendet worden ist und da kann Integrität entsprechend helfen.

Es können aber natürlich auch Daten manipuliert werden, die ich herunterlade. Wenn ich Pech habe, habe ich so etwas wie eine Ransomware heruntergeladen. So heißt eine Software, die

ich auf meinen Computer lade und wenn ich die dann ausführe, wird der komplette Festplatteninhalt verschlüsselt und ich werde dann erpresst. Für die Entschlüsselung müsste ich Lösegeld an die Hackerinnen und Hacker zahlen. Das hat natürlich Konsequenzen, wenn das Backup fehlt. Das Blöde ist, dass die Cyberkriminellen auch keinen Halt machen vor kritischen Infrastrukturen, wie das letztens auch bei der Uni-Klinik Düsseldorf passiert ist. Da war eine Ransomware aktiv und dann musste das Krankenhaus komplett von digital auf analog umstellen. In diesem Fall waren wirklich Menschenleben gefährdet: Wir haben eine Pandemie, *(es besteht)* sowieso schon *eine* hohe Belastung für Krankenhäuser und dann kommt jetzt noch die Ransomware dazu. Womit wir auch bei der Verfügbarkeit wären: Die ist dann gefährdet, weil ich vielleicht nicht mehr alle Patientinnen und Patienten bedienen kann.

Wenn wir das Thema Integrität ein bisschen weiter greifen, lässt sich das natürlich auch auf das aktuelle Thema Social Media/Fake News beziehen. Was ist denn noch wahr, was ist falsch? Wenn Akteurinnen und Akteure die Möglichkeit haben, Falschnachrichten oder Desinformation zu verbreiten, dann bedroht das natürlich auch die Integrität von Wahlen beispielsweise.

Zugriffskontrolle und Authentizität

Aus Sicht von Banken ist es wichtig zu wissen, dass sich die legitime Person bei der Online-Bank einloggen möchte. Weil sonst, natürlich, finanzieller Schaden entsteht.

Bei der Authentizität geht es um die Fragen: *Habe ich es mit dem richtigen Kommunikationspartner auf der anderen Seite zu tun? Rede ich also mit meiner Bank oder habe ich aus Versehen eine Phishing-Seite angeklickt?* Und dann ist vielleicht das Geld weg, wenn ich auf der Phishing-Seite meine Online-Bankingdaten angegeben habe. Um Kundinnen und Kunden vor solchen Angriffen zu schützen, gibt es mittlerweile die europäische PSD2-Richtlinie. Da wurde Zwei-Faktor-Authentifizierung verpflichtend für Online-Banking vorgeschrieben, d. h., ich logge mich bei meiner Online-Bank ein und werde dann zusätzlich nach einem weiteren Authentifizierungsfaktor gefragt. Das ist beispielsweise ein Zahlencode, den ich an mein Handy geschickt bekomme. Für erhöhte Sicherheit muss ich den dann noch eingeben.

Der Security-Usability-Tradeoff-Mythos

Tagesschau.de hat auch über die PSD2-Richtlinie berichtet und im zugehörigen Artikel[2] war ein interessanter Satz dabei. Zitat:

> *„Überweisungen und Online-Käufe sind künftig etwas **komplizierter** – aber hoffentlich auch sicherer."*

Dieser Satz spiegelt diese typische Denkweise wieder, die manche offensichtlich im Bereich IT-Sicherheit haben, nämlich: Wenn ich die Sicherheit erhöhe, habe ich automatisch weniger Usability.

Mit diesem Mythos haben renommierte Forscherinnen und Forscher im Usable-Security-Bereich aufgeräumt in ihrem Artikel zum Thema „The Security-Usability Tradeoff Myth"[3] im IEEE Security & Privacy Magazine.

Darin geht es um dieses typische Klischee: *Ich habe mehr Sicherheit, bedeutet das, dass ich weniger Usability habe?* Die Autorinnen und Autoren sagen: Nein! Es funktioniert nicht, weil, wenn ich jetzt die Sicherheit komplett hoch setze, aber dann meine Userinnen und User die Sicherheitsmechanismen nicht richtig anwenden können, dann schlägt die Sicherheit fehl.

Wie bei der E-Mail-Verschlüsselung, auch so ein Thema, …

Wer von Euch, von Ihnen, hat schon mal PGP benutzt? Ich bin richtig dran verzweifelt bei der Konfiguration, leider. Aber das ist auch so ein Beispiel. Ich kann hier sehr viel Sicherheit erreichen, muss aber genau wissen, was ich einstellen muss. PGP lässt sich aber nicht so leicht und intuitiv bedienen und wenn ich einen Button falsch klicke, schlägt die Sicherheit fehl. Das heißt: Weniger Usability bedeutet nicht automatisch mehr Sicherheit und da gibt es genügend Studien, die das auch entsprechend gezeigt haben.

Jetzt gehen wir mal in den umgekehrten Fall rein. *Wenn ich mehr Usability habe, bedeutet das, dass ich weniger Sicherheit habe?* Die Autorinnen und Autoren sagen: Natürlich nicht, weil ich ohne Sicherheitsmechanismen so gut wie keine App bedienen kann. Wenn ich Online-Banking mache, muss ich mich irgendwie noch auf meiner Webseite einloggen. Das heißt, irgendein Sicherheitsfeature muss ich dabeihaben, sonst klappt das nicht.

Und es gibt ja genügend Fälle in der Praxis, bei denen wir sehen können, dass das eben nicht funktioniert. Deswegen sind die Forscherinnen und Forscher auf den Konsens gekommen, das Ziel soll am Ende sein, eine *reflektierte Ausgewogenheit* zu schaffen. Denn wenn ich Sicherheitsfunktionen gebrauchstauglich mache, dann nutzen sie meine Nutzerinnen und Nutzer wahrscheinlicher richtig, womit wir insgesamt die Sicherheit erhöhen. Und das ist das Thema, worüber wir eben sprechen: Usable Security. Natürlich gibt es auch Usable Privacy, die sich mehr auf Privatheit bezieht. Es geht aber grundsätzlich darum: Wir haben diese technologischen Faktoren, d. h. Sicherheits- oder Privatheitsfunktionen, und die menschlichen Faktoren und gucken eben, wie Menschen darauf reagieren. Die akademischen Forschungsgebiete sind da ziemlich groß, beispielsweise: Wie authentifiziere ich Personen? Phishing – wie gehe ich dagegen vor? Wie sieht das mit Social Media und der Privatsphäre aus? Email Privacy, wie schütze ich mich vor Massenüberwachung? Wie verbinde ich Geräte usw. Das ist wirklich ein breites Forschungsgebiet. Wir gehen in den näheren Beispielen mehr auf Usable Security ein aus Zeitgründen. Es gibt aber ähnliche Beispiele, die auf Privacy zutreffen.

The Elephant in the Room

Wenn wir jetzt mal aus der IT-Sicherheitsperspektive agieren, stehen wir natürlich auch vor Herausforderungen, denn wir haben ein offensichtliches Problem in der IT-Sicherheit. Das Problem ist nämlich einerseits technisch: IT-Sicherheitsmechanismen sind schwer zu erklären und nicht so leicht zu verstehen. Andererseits ist Security immer eine Nebenaufgabe.

Wir haben beispielsweise einen Cloud-Speicher, bei dem ich meine Daten hochladen möchte, und dann, während ich diese Aufgabe erledigen möchte, kommt irgendein Sicherheitsmechanismus dazwischen. Beispielsweise die Passwortabfrage. Wir haben ja eigentlich ein anderes Ziel und das ist besonders dann schwierig, wenn wir im Stress sind. Jeder von uns hat mal einen schlechten Tag oder ist gerade krank und muss jetzt irgendwie Aufgaben erledigen und dann kann es richtig schwierig werden. Gerade, wenn ich dann in diesen Momenten nicht richtig aufpasse, weil ich vielleicht einen schlechten Tag habe, klicke ich vielleicht aus Versehen auf eine Phishing-Mail und gebe Daten preis, die ich nicht preisgeben wollte, wie Firmendokumente oder Ähnliches. Fehler sind menschlich, das kann schon mal passieren.

Ebenso dürfen wir nicht vergessen: Angreifende sind nun mal Akteure, die unsere Daten haben wollen. Dazu nutzen sie menschliche Eigenschaften aus. Die wollen uns psychologisch dazu bringen, dass wir beispielsweise auf einen Phishing-Link klicken und unsere Logindaten preisgeben. Und da müssen wir versuchen, mit Usable Security die Software widerstandsfähig dagegen zu machen.

Ein paar Beispiele, die noch mit reinkommen: Wir haben beschränkte kognitive Fähigkeiten, wir können uns jetzt nicht hunderte Passwörter merken oder gewöhnen uns vielleicht auch an Dinge, Beispiel Browser-Warnungen: Wenn zu häufig eine Meldung kommt wie „Ihre Webseite ist unsicher“ und wir zum hundertsten Mal gelernt haben, *„ok, das ist nicht wichtig, jetzt klick ich einfach auf ‚Ignorieren‘“,* dann klicke ich immer auf „Ignorieren“. Dann habe ich mich schon so daran gewöhnt, dass ich das automatisiert mache und ich nicht mehr drüber nachdenke. Und dann kommt vielleicht eine böse Gegenseite und mogelt uns auch so eine Meldung unter. Wir klicken dann auch instinktiv auf „Ignorieren“ und schwupp – haben die Angreifenden ihr Ziel erreicht.

Deswegen: Software entsprechend widerstandsfähig bauen. Wir dürfen auch nicht vergessen, jeder Mensch ist anders. Jeder hat ein anderes Sicherheitsempfinden, wir empfinden Risiken vielleicht anders, wir haben einen anderen Wissensstand bezüglich IT-Sicherheit und das müssen wir später alles beachten, wenn wir Usable-Security-Sachen behandeln wollen.

Sind die User an allem schuld?

Passend dazu gibt es auch typische Sachen, mit denen wir mal aufräumen wollen.

Beispielsweise in der Firmenkommunikation hat eine bekannte Firma folgenden Satz gebracht: „Users are the weakest link in security“ (Die User sind das schwächste Glied in der IT-Sicherheit). Hier wurde dann auch erwähnt, 63 % der Passwörter, die verwendet wurden, sind schwach oder wurden geklaut. Ja, aber, wenn wir uns das genauer angucken: Sind wir wirklich das schwächste Glied in der IT-Security? Sind wir die Feinde, die das Problem sind?

Vom Britischen BSI-Pendant, dem NCSC *(National Cyber Security Center),* hat Ciaran Martin dieses Thema später in einem Vortrag aufgegriffen:

> *„Lassen Sie uns ernsthaft versuchen, den Menschen in all dem zu verstehen. Lassen Sie uns aufhören, Unsinn darüber zu reden, dass der Mensch das schwächste Glied in der Cybersicherheit sei. Es ist ein bisschen so, als würde man sagen, das schwächste Glied in einer Sportmannschaft seien alle Spieler.“*[4]

Und das trifft es eigentlich gut auf den Punkt. Denn nur wenn wir alle zusammenarbeiten, dann können wir die Sicherheit verbessern, und ich denke, ein Fußballteam mit lauter Egoisten spielt nicht so gut. Dieses Thema hatten schon vor 20 Jahren die Forscherinnen Anne Adams und Angela Sasse in ihrer Publikation „Users are not the enemy“[5] beschrieben. Dieses Feindbild des „dümmsten anzunehmenden Users“ ist totaler Quatsch und mit diesem Klischee muss aufgeräumt werden. Seitdem gibt es diese Denkweise der Usable Security und Privacy. Dank der Forscherinnen, die das damals in ihrem – etwas zugespitzt formuliert – Brandbrief dargestellt haben. Auch vom NCSC hat Emma W., eine Mitarbeiterin, auch noch mal einen Vortrag[6] zu diesem Thema gebracht, in dem sie formulierte: „Security must work for people. If security doesn't work for people, it doesn't work.“ (Wenn die Security nicht für Menschen funktioniert, wird sie insgesamt keinen Effekt haben.) Der Titel dieses Vortrags hieß: „People: The Strongest Link“, also Menschen, das stärkste Verbindungsstück. Wir würden das allerdings nochmal ein bisschen genauer formulieren: Empower people to become a strong link, also Menschen befähigen, ein starkes Verbindungsstück zu werden. Und das ist genau, was wir im Bereich der Usable Security und Privacy eben machen. Wir nehmen uns Sicherheitsmechanismen, evaluieren die nach gängigen Usability-Metriken und stellen dann fest, dass sie vielleicht gar keinen Sinn machen, wie die Schranke in Abbildung 3, die alle Personen umfahren.

Abbildung 3: Usability Evaluation von Sicherheitsmechanismen

Wenn man jetzt diese Schranke sieht, bevor sie dann fertig geworden ist und alle drumherum fahren, dann müssen wir uns überlegen: Ok, können wir das vielleicht anders designen? Deswegen: Im Entwicklungsprozess diese Mechanismen testen und schauen, wie Menschen darauf reagieren. Sozusagen *Security and Usability by Design.* Und dann werden die Sicherheitsmaßnahmen effektiver.

Wenn wir uns jetzt nochmal diesen Satz von vorhin anschauen, können wir „Users are the weakest Link in Security“ ganz klar streichen. Weil das Problem, das wir hier haben, nicht die Nutzerinnen und Nutzer sind, sondern die Passwörter, die gewählt worden sind. Die sind schwach, aber vielleicht gab es überhaupt keine Warnmeldung, um zu sagen: Hey, da gibt es ein Datenleck, und jetzt bitte das Passwort ändern. Das ist vielleicht einer der Gründe und deshalb müssen wir hier den Nutzerinnen

und Nutzern helfen, damit sie die Sicherheitsmechanismen richtig anwenden können.

Forschungsbereich Passwörter

Und wo wir schon beim Thema Passwörter sind, gehen wir ein bisschen mehr in den Bereich Personenauthentifizierung rein. Das ist auch der Bereich, in dem ich forsche. Es geht um textbasierte Passwörter.

Klar, Passwörter werden von uns allen benutzt, manche lieben sie, manche hassen sie, aber womit wir uns auf jeden Fall sicher sein können: wir werden sie auf längere Zeit nicht mehr weg bekommen aus dem Netz aus folgenden Gründen: Einerseits aus der Nutzerinnen- und Nutzer-Perspektive: wenn ich so ein Formular sehe, dann weiß ich genau, was zu tun ist. Das können Sie wahrscheinlich Ihrer Oma zeigen oder Ihren Großeltern, ihren Eltern, wem auch immer, die wissen ganz genau, was zu tun ist, wenn sie dieses Formular mit Nutzername und Passwort sehen.

Und aus der Entwicklerinnen- und Entwickler-Perspektive ist das auch relativ einfach zu lösen. Wir müssen da nur zwei Zeichenkombinationen prüfen und dann bin ich drin. Und natürlich ein weiterer Vorteil von Passwörtern: unser Gehirn ist nicht hackbar, momentan zumindest noch nicht, und deswegen sind Passwörter erst einmal noch nicht weg zu bekommen. Wir haben aber trotzdem natürlich dieses Sicherheitsproblem: Wenn ich zu lange Passwörter wähle, kann ich sie mir schwer merken, und wenn ich sie zu kurz wähle, kann ich sie mir leichter merken, sie sind aber auch leichter hackbar. Und in der letzten Zeit sind auch weitere Sicherheitsrisiken dazu gekommen. Das sind Passwörter, die geklaut worden sind, beispielsweise von größeren Internetseiten. Das haben wir am Anfang der Präsentation schon gesehen.

Beispielsweise sind von LinkedIn riesige Datensätze mit E-Mail-Adressen und Passwörtern abhandengekommen. Wenn wir jetzt hacken würden, würden wir einfach diese Datensätze kaufen von irgendwelchen Darknet-Marktplätzen oder wo auch immer her. Dann gehen wir automatisiert diese Nutzernamen-Passwort-Kombinationen durch, können das ja auf einer anderen Webseite mal probieren und dann kommen wir vielleicht in einige Accounts rein. Wir sind halt Menschen und nutzen Passwörter auch gerne mal wieder. Gegen diese Angriffsmethoden müssen wir natürlich vorgehen. Wir müssen schauen: Wie kann ich die Sicherheit von Passwörtern erhöhen, um meine Nutzerinnen und Nutzer zu schützen auf meiner Webseite, dass eben nicht so ein Angriff passieren kann?

Passwortrichtlinien und ihre Probleme

Da gibt es beispielsweise Passwortrichtlinien, so Sachen wie „benutzen Sie ein Passwort mit Groß- und Kleinschreibung, bauen Sie Sonderzeichen ein und machen Sie noch Zahlen rein, viel-

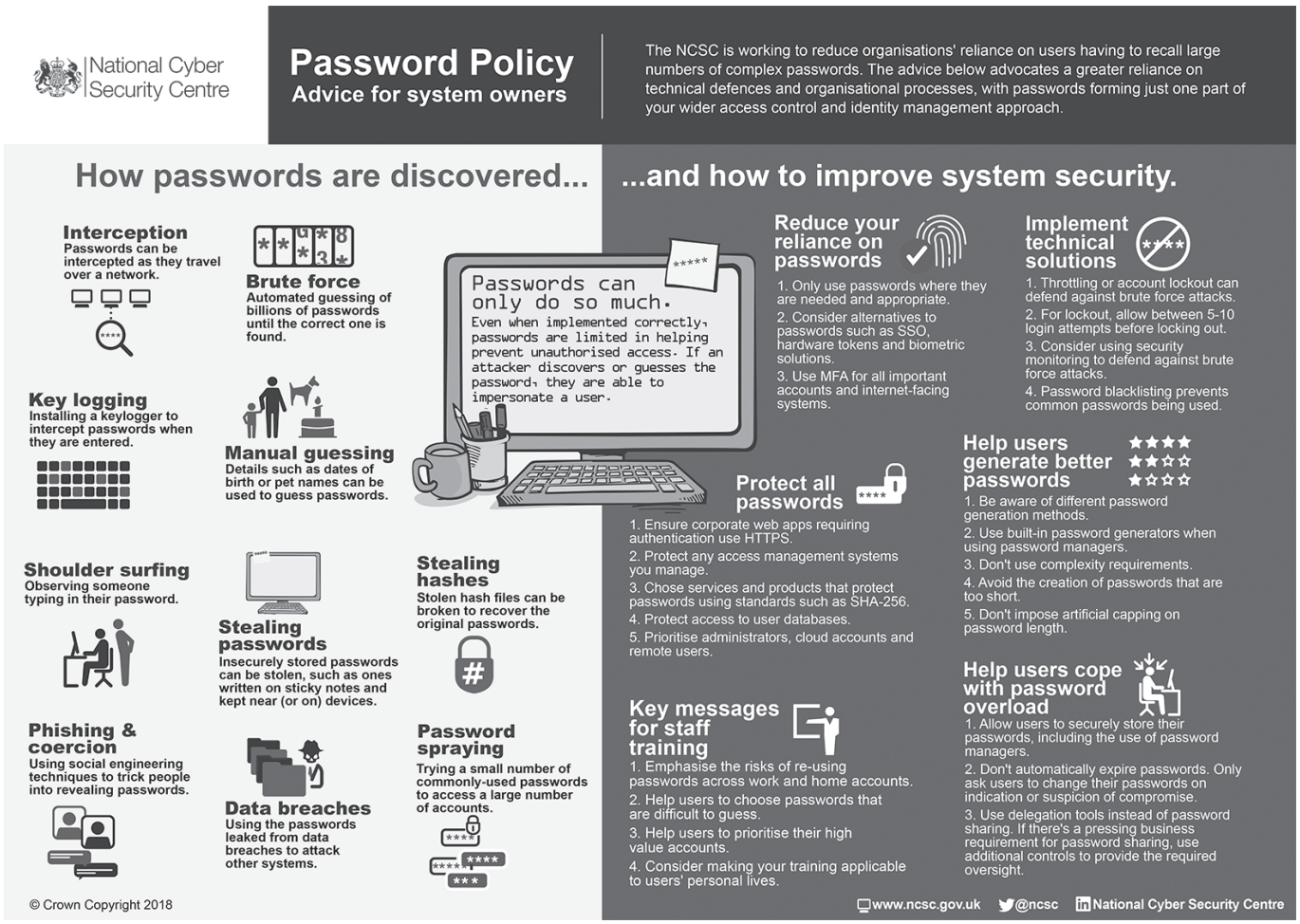


Abbildung 4: Password Security Info Sheet des NCSC.[9] © Crown Copyright NCSC 2018. Lizensiert unter Open Government Licence v3.0 OGL

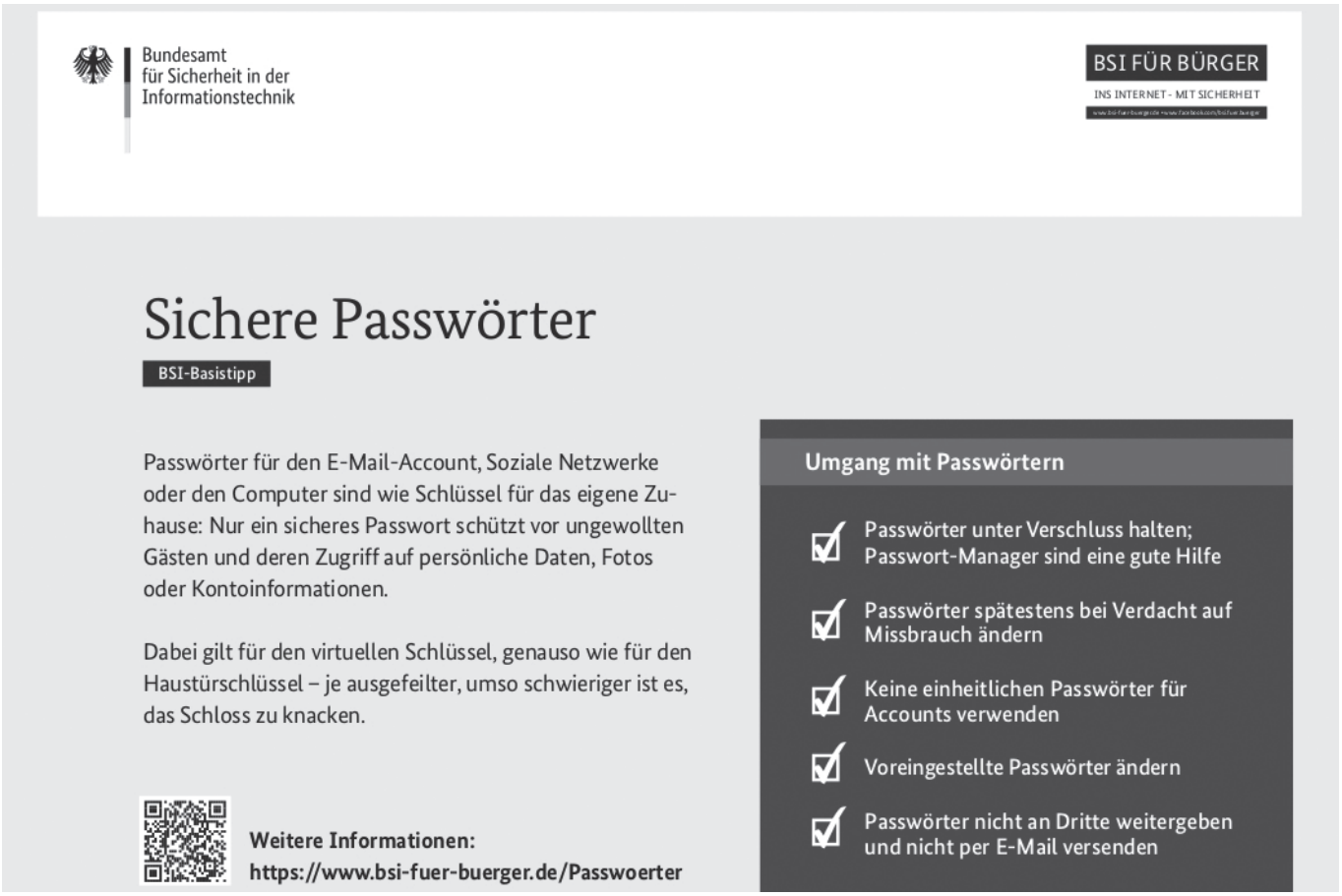


Abbildung 5: Ausschnitt aus dem Faktenblatt „Sichere Passwörter" des BSI[8] © BSI

leicht noch ein Einhorn-Emoji rein und dann am besten noch das Passwort alle drei Monate ändern". Das ist so etwas, was man auf Webseiten sehr häufig liest.

Die Praxis zeigt aber: das funktioniert nicht. Wenn man Passwortrichtlinien nämlich mal evaluiert hat in der Wissenschaft, sieht man: Wenn ich Angreifender bin, dann weiß ich ganz genau, wonach ich suchen muss, weil ich ja schon weiß, welche Zeichen im Passwort drin sein müssen. Das heißt: ich spare mir viel Ratezeit. Dazu kann ich mir solche Passwörter nur schwer merken und vor allem lösen sie das Hauptproblem ja gar nicht. Sie verhindern weder Keylogging noch Phishing und wir wissen ja, es ist der effektivste Weg, Menschen mit Ihren Schwächen anzugreifen.

Das heißt: Es ist eine Luftnummer, weshalb man die Passwörter nicht mehr alle drei Monate ändern sollte. Mittlerweile sagt das auch das BSI, nachdem es die amerikanischen und britischen Behördenpendants schon lange empfohlen haben.

In der Praxis, für diesen Fall, was machen wir dann, wenn wir uns Passwörter schwer merken können? Genau, wir schreiben sie auf Post-Its oder malen sie auf die Pinnwand drauf! Und wenn ich dann Pech habe und ein Fernsehteam bei mir reinkommt und dann diese Wand abfilmt, dann haben wir das Problem, dass wir eventuell gehackt werden, wenn Online-Dienste keine weiteren Sicherheitsmaßnahmen einbauen. Nicht zu vergessen: Vergessene Passwörter können auch finanzielle Folgen haben, wie man das bei einem bekannten Autohersteller sehen konnte. Die hatten nämlich einen externen Dienstleister bestellt, der für die Passwortzurücksetzung zuständig war und dann für jede Rücksetzung Geld verlangte. Blöderweise haben die Mitarbeiterinnen und Mitarbeiter, weil sie alle drei Monate ihr Passwort ändern mussten, sehr oft ihr Passwort vergessen und letzten Endes war das dann teuer. Eine Million Euro Extra-Ausgaben nur durch die Passwortzurücksetzungen.

Wenn Sie und Ihr da noch Interesse dran habt, da noch ein bisschen näher rein zu schauen: Es gibt zu Passwörtern vom NCSC aus Großbritannien noch ein Infosheet, auf welchem man die Empfehlungen für Passwörter nachschauen kann (Abbildung 4). Da steht auch nochmal „blacklist the most common password choices". D. h., hier ist auch nochmal die Empfehlung, nicht die häufigsten, beliebtesten Passwörter zu wählen für einen Onlinedienst.[7] Beim BSI gibt es auch noch eine ähnliche Broschüre[8], da dann einfach mal reinschauen (Abbildung 5).

Zwei-Faktor-Authentifizierung als Allheilmittel?

Also, das haben wir abgehakt: Password Policies – keine so gute Idee, um die Sicherheit zu erhöhen. Aber was ist denn jetzt mit Zwei-Faktor-Authentifizierung, werden vielleicht manche jetzt im Podium denken? Klar, es wird natürlich von vielen Online-Diensten angewendet. Ich logge mich mit Nutzernamen und Passwort ein. Dann werde ich nach einem zusätzlichen Authentifizierungsfaktor gefragt, also dieser SMS-Code beispielsweise. Oder ich klicke auf einer App irgendwo drauf. Wenn dieser Beweis erbracht wurde, dann bin ich drin auf der Webseite.

Spätestens seit dem „Bundes-Hack“ – manche erinnern sich vielleicht noch letztes Jahr daran, als von Politikern und Prominenten Konversationen gehackt und öffentlich zugänglich ins Internet gestellt worden sind – da war dann das Echo in der Politik groß, nach dem Motto: „wir brauchen eine Zwei-Faktor-Authentifizierungspflicht!“ Ich weiß gar nicht, ob viele Politiker mittlerweile überhaupt noch wissen, was Zwei-Faktor-Authentifizierung ist. Das Thema ist irgendwie in Vergessenheit geraten. Vielleicht liegt das auch daran, dass das offensichtliche Problem nicht angesprochen wurde: Die Akzeptanz von Zwei-Faktor-Authentifizierung ist recht gering, sofern auf der Website keine sehr sensiblen Daten im Spiel sind, wie z. B. bei Online-Banking. Selbst Google musste zugeben, dass weniger als 10 % der Nutzerinnen und Nutzer bei Google überhaupt Zwei-Faktor-Authentifizierung aktiviert haben. Um die restlichen 90 % der Personen zu schützen, die keine Zwei-Faktor-Authentifizierung aktiviert haben, sollten entsprechende Maßnahmen ergriffen werden.

Risikobasierte Authentifizierung (RBA)

Eine davon wäre risikobasierte Authentifizierung. Die erhöht nämlich die Sicherheit im Vergleich zu Nur-Passwort-Authentifizierung und erhöht gleichzeitig die Usability.

Es funktioniert wie folgt: Ich habe meinen Anmeldenamen und mein Passwort und wenn ich das Login-Formular absende, übermittle ich automatisch zusätzlich Metadaten, die sowieso schon in dem Kontext vorhanden sind, beispielsweise: Welche IP-Adresse habe ich, welches Gerät nutze ich zum Einloggen, welchen Browser? Und basierend darauf wird im Hintergrund ein Risiko berechnet. Basierend auf meinen vorherigen Login-Versuchen, wie wahrscheinlich ich das jetzt bin oder wie hoch das Risiko ist, dass das jetzt ein Hacking-Angriff ist. Das Risiko wird normalerweise in niedrig, mittel und hoch unterteilt.

Wenn wir jetzt mal den Fall für niedriges Risiko anschauen. Ich bin jetzt beim FIfF und logge mich aus Bremen ein, mit einem Gerät, das ich sonst immer benutze. Und wenn das Verhalten so wie immer ist, komme ich einfach in meine Webseite rein und werde nicht nach zusätzlichen Authentifizierungsfaktoren gefragt.

Und jetzt gehen wir mal an einen Ort, wo ich mich persönlich relativ selten aufhalten würde. Und da ist sich das System nicht mehr ganz so sicher, weil ich mich vorher noch nie aus dem Land eingeloggt habe und ein Gerät benutze, was ich sonst nie benutzt habe, dann ist sich die Website nicht so sicher: Ist das wirklich die richtige Person, die sich hier einloggen möchte? Und dann fragt mich die Website nach einer zusätzlichen Authentifizierung. Das kann beispielsweise eine E-Mail-Adresse sein, die ich dann noch einmal bestätigen muss. Das heißt, ich muss mich nochmal in den E-Mail-Account einloggen und wenn ich diesen Beweis erbracht habe, komme ich auf die Webseite drauf.

Und hier sieht man den Unterschied zur Zwei-Faktor-Authentifizierung im klassischen Sinne: Wir werden nicht immer nach zusätzlicher Authentifizierung gefragt. Diese Technologie wird empfohlen vom NIST, also dem amerikanischen Pendant zum BSI, in den NIST Digital Identity Guidelines[10] – wenn es noch nicht gelesen wurde, einfach mal reinschauen. Da sind sehr viele Usable Security und Privacy Metriken drin, das ist ganz interessant zu lesen.

Große Onlinedienste setzen RBA ein, Facebook, Google, LinkedIn und weitere. Wir wissen auch durch unsere Forschung, dass RBA von Anwendern als gebrauchstauglicher angesehen wird als vergleichbare Zwei-Faktor-Authentifizierungsmethoden und auch die Sicherheit wird vergleichbar wahrgenommen. Darüber hinaus wissen wir, dass RBA in der Praxis sehr selten nach der zusätzlichen Authentifizierung fragt. Selbst dann, wenn mehr als 99,45 % intelligenter Angriffe blockiert werden. Also Angriffe mit Kenntnis zu den Anmeldedaten des Opfers sowie dessen typischem Standort (Stadt, Land), Browser und Gerät. Abbildung 6 zeigt Beispiele von Dialogen, wenn RBA aktiv wird.

Zum Thema RBA haben wir eine Info-Webseite aufgesetzt: *riskbasedauthentication.org*. Da sind viele Studien dabei, unter an-

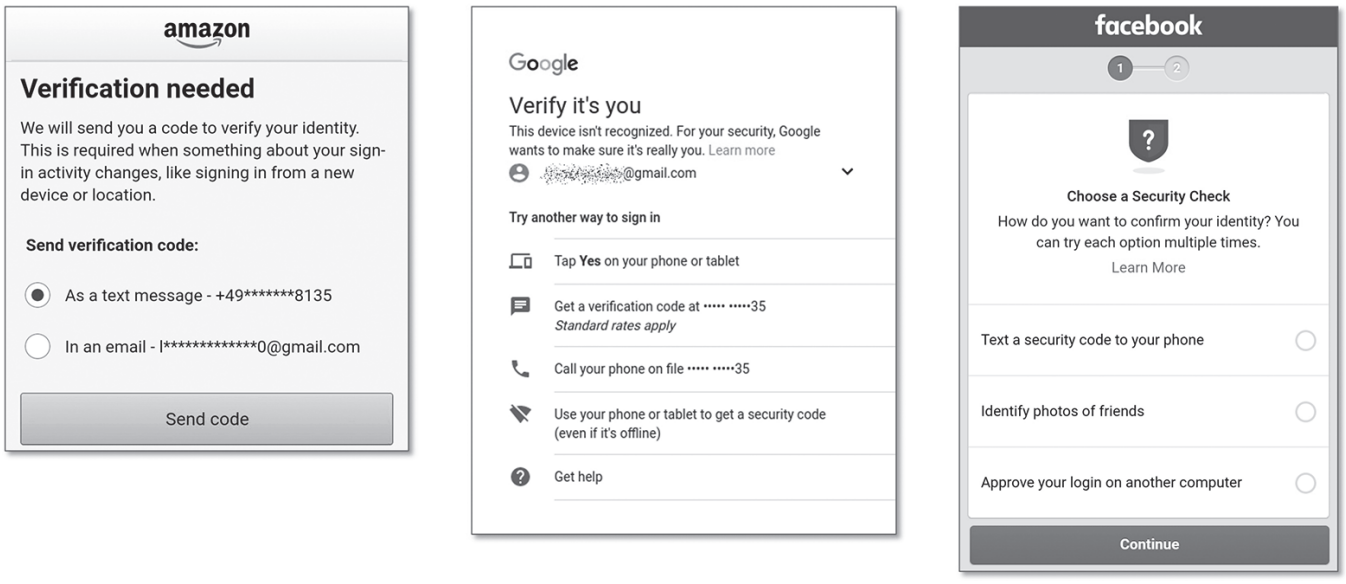


Abbildung 6: Dialoge während risikobasierter Authentifizierung. © Stephan Wiefling 2019

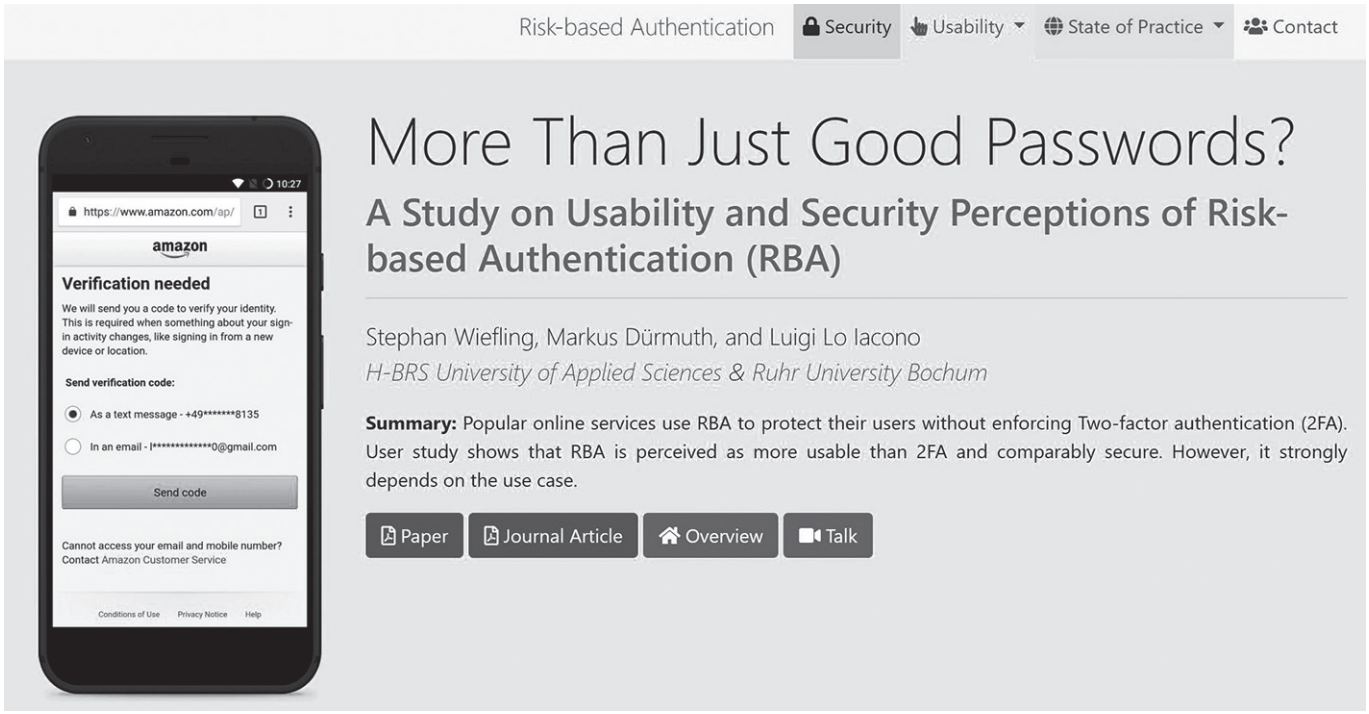


Abbildung 7: A Study on Usability and Security Perceptions of Risk-based Authentication (RBA).[11] *© Stephan Wiefling 2020*

derem auch eine ganz neue Studie (Abbildung 7), in der wir die Usability von RBA genauer untersucht haben.

Der IT-Security-Guru Bruce Schneier hat auch darüber berichtet, das ist ganz lustig gewesen. Er fand es auf jeden Fall „interesting". Also wenn das kein Grund ist, rein zu schauen, dann weiß ich auch nicht!

Usable Security & Privacy in die Praxis bringen

Aber wir kommen jetzt nochmal generell zu Usable Security und Privacy hin. Irgendjemand muss es ja in die Praxis umsetzen und das sind meistens Entwicklerinnen und Entwickler. Wie können wir diesen Personen helfen, um Usable Security und Privacy in Software einzubauen? Dafür haben wir ein Tool gebaut, die USecureD-Plattform (Abbildung 8).

Da haben wir beispielsweise für alle möglichen Kategorien aufgelistet, was es so gibt an Sachen, die man als Programmiererin und Programmierer gestalten kann. Wenn wir uns beispielsweise Warnmeldungen anschauen wollen, ist da genau aufgelistet, wie der aktuelle Forschungsstand ist und was die Empfehlungen sind: Wie soll ich eine Warnmeldung gestalten, damit das dann auch effektiv zu einem zufriedenstellenden Ergebnis führt, dass Sicherheitsmethoden richtig angewendet werden?

Da gibt es auch eine Übersicht, wo wir uns durchklicken können. Wenn wir z. B. die Warnmeldungen haben, können wir draufgehen und dann werden auch noch andere Kategorien angezeigt, die verwandt sind. Das ist ein ganz gutes Nachschlagtool, um einfach eine Übersicht zu haben: Was ist denn aktuell populär und was ist der aktuelle Stand der Forschung? Einfach mal vorbei schauen lohnt sich an der Stelle.

Abbildung 8: Oberfläche der USecureD-Plattform.[12] *© DAS-Group TH Köln 2017*

Zusammenfassung

Was sollten wir jetzt von dem Vortrag mitgenommen haben?

Zunächst mal Security ohne Usability geht auf jeden Fall nicht. Ausgewogenheit ist gefragt, der Usability-Security Tradeoff Myth – mehr Sicherheit = weniger Usability – ist Quatsch.

Und ebenso: Empower people to become a strong link in Security, d. h., nur zusammen können wir wirklich stark werden.

Und dann möchten wir noch ein paar Literaturtipps am Ende mitgeben:

- „Usable Security: History, Themes and Challenges", Simson Garfinkel und Heather Lipford, 2014
- „Security and Usability: Design Secure Systems that People can use", Lorrie Faith Cranor und Simson Garfinkel, 2005
- Literaturempfehlungen des Arbeitskreises Usable Security & Privacy der German UPA *https://germanupa.de/arbeitskreise/arbeitskreis-usable-security-privacy/unsere-literaturempfehlungen*

Und es gibt noch Konferenzen, auf denen aktuelle Forschungsergebnisse vorgestellt werden.

Da gibt es das Symposium of Usable Privacy and Security (SOUPS)[13]. Da ist auch viel Open Access dabei, d. h., es kostet auch nichts, es ist keine Paywall dazwischen. Das kann ich empfehlen, alle anderen, die auf der Liste sind, auch. Das Privacy Enhanced Technologies Symposium (PoPETs)[14] ist mehr auf Usable Privacy angewandt und mehr auf dem Usability Fokus ist dann die Conference on Human Factors in Computing Systems (CHI)[15].

Es gibt auch noch wissenschaftliche Workshops zum Thema:

Der deutsche Usable Security & Privacy Workshop[16] findet immer auf der „Mensch und Computer" statt. In Europa gibt es den European Workshop on Usable Security (EuroUSEC)[17], international die USEC[18]. Da treffen sich Forscherinnen und Forscher aus dem Fachbereich und tauschen sich aus. Das ist ganz hilfreich, um Kontakte in die Usable-Security-Szene zu bekommen.

Damit sind wir dann auch am Ende vom Vortrag angekommen. Ich hoffe, dass ich Sie und Euch für das Thema Usable Security und Privacy begeistern konnte. Weitere Infos haben wir auch auf unserer Webseite *das.h-brs.de* von unserer Gruppe für Daten- und Anwendungssicherheit der Hochschule Bonn-Rhein-Sieg, wo wir die neuesten Ergebnisse zeigen, oder natürlich *riskbasedauthentication.org*, unsere RBA-Infoseite.

Wenn es jetzt noch Fragen gibt, freue ich mich auf die, die gleich in den entsprechenden Chat kommen, aber ansonsten bin ich auch per E-Mail[19] erreichbar oder Twitter[20]. Wenn Sie Fragen haben zu dem Thema, sagen Sie einfach Bescheid und ich freue mich da auf eine Rückmeldung und ansonsten vielen Dank fürs Zuhören.

Anmerkungen und Referenzen

1 *McCandless D, Evans T, Barton P, Starling S, Geere D (2019) World's Biggest Data Breaches & Hacks. Information is Beautiful, 1. April 2019. https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/*
2 *https://web.archive.org/web/20190913083203/ https://www.tagesschau.de/wirtschaft/online-banking-zwei-faktor-methode-101.html*
3 *Sasse MA, Smith M, Herley C, Lipford H, Vaniea K (2016) Debunking security-usability tradeoff myths. IEEE Security & Privacy 14(5):33–39. doi:10.1109/MSP.2016.110*
4 *NCSC (2017) Ciaran Martin's speech to CBI. 13. September 2017. https://www.ncsc.gov.uk/speech/ciaran-martins-speech-cbi*
5 *Adams A, Sasse MA (1999) Users are not the enemy. CACM 42(12):40–46. doi:10.1145/322796.322806*
6 *https://www.youtube.com/watch?v=u6x9C7t_41s*
7 *https://ncsc.gov.uk/guidance/password-guidance-simplifying-your-approach*
8 *https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Checklisten/sichere_passwoerter_faktenblatt.pdf?__blob=publicationFile&v=1*
9 *https://www.ncsc.gov.uk/files/password_policy_infographic.pdf*
10 *Tech. Rep. NIST-SP 800-63b 2017*
11 *https://riskbasedauthentication.org/usability/perceptions/*
12 *https://das.h-brs.de/usecured*
13 *https://www.usenix.org/conference/soups2020*
14 *https://www.petsymposium.org*
15 *https://chi2020.acm.org*
16 *https://das.h-brs.de/workshops/*
17 *https://eusec20.cs.uchicago.edu/*
18 *Workshop on Usable Security and Privacy. http://www.usablesecurity.net/USEC/usec21/*
19 *Stephan.wiefling@h-brs.de*
20 *@swiefling*

Stephan Wiefling

Stephan Wiefling ist wissenschaftlicher Mitarbeiter in der Data and Application Security Group der Hochschule Bonn-Rhein-Sieg. Seine Forschungsschwerpunkte liegen in den Bereichen der Authentifizierung und Usability. E-Mail: *Stephan.wiefling@h-brs.de*. Twitter: *@SWiefling*

Zinaida Benenson

Menschengerechte IT-Sicherheit

Vortrag auf der FIfF-Konferenz am 14. November 2020

Transkription und Überarbeitung: Sylvia Johnigk und Eberhard Zehendner.

Gestaltungseffektive IT-Sicherheit erfordert die Berücksichtigung der Fähigkeiten der nicht fachkundigen Nutzenden. Leider sind dabei die Anforderungen an die Nutzenden oft unrealistisch. Ihnen wird unsicheres Verhalten vorgeworfen, ohne zu fragen: Sind sie überhaupt in der Lage, sich „sicher" zu benehmen? Statt der zum Scheitern verurteilten Versuche, die Nutzenden durch Sensibilisierung und Schuldzuweisung an die IT-Systeme anzupassen, sollten die IT-Systeme an sie angepasst werden. Wie das gelingen könnte, wird in diesem Beitrag dargestellt.

Und insbesondere auch: Was passiert, wenn die Menschen angegriffen werden? Denn das kam bisher, denke ich, nicht so genau oder nicht so oft zur Sprache. Ich werde zwei Studien vorstellen, die wir in meiner Forschungsgruppe durchgeführt haben. In einer geht es um Phishing und in der anderen um Antivirus-Meldungen. Es hat sich herausgestellt, dass das nicht so ganz menschengerecht ist. Und dann werde ich versuchen, ein bisschen zu erklären oder vorzustellen, was denn menschengerechte Sicherheit sein könnte.

Die Phishing-Studie

Sie haben bestimmt schon von *Spear Phishing* gehört. Das ist gezieltes personenbezogenes Phishing, kann manchmal auch Namen oder Adressen der Empfänger:innen enthalten, und manchmal ist es auch abgestimmt auf die Umstände, in denen sie leben, und hat dann einen interessanten oder plausiblen Inhalt. Das Problem ist, dass die Nachricht versucht, per Anhang oder Link eine Malware auszuführen. Viele Angriffe, wie zum Beispiel *Advanced Persistent Threats* (APT) oder *Ransomware,* beginnen mit Spear Phishing. Das wird in den Firmen gefürchtet, insbesondere auch im Online-Banking-Bereich.

Wir haben uns in unserer Studie gefragt, welche Gründe es fürs Anklicken gibt, wenn Leute so etwas bekommen. Denn man hört oft gerade von Sicherheitsexpert:innen: „Oh, mein Gott, wie kann man auf so etwas klicken?" Und genau das wollten wir herausfinden. Wir haben dazu zwei Experimente durchgeführt. Ich werde jetzt einfach kumulativ Ergebnisse vorstellen. 2016 habe ich auf der *Black Hat USA* einen Vortrag[1,2] dazu gehalten, darin wird es ein bisschen mehr erklärt.

Die Phishing-Nachricht

Abbildung 1 zeigt den Text einer E-Mail, die wir sieben Tage nach Silvester an rekrutierte Teilnehmer:innen unter den Studierenden unserer Universität verschickt haben. *Hey wie gehts? Silvester war ja echt der hammer!* Und da gab es einen Link, der eigentlich ziemlich verdächtig ist: da war einfach eine IP-Adresse, die zur Uni gehört, zu unserem Lehrstuhl, und eine personalisierte ID für die User. Wenn sie darauf geklickt haben, erschien eine Webseite mit der Meldung „access denied". Diese Nachrichten wurden mit unterschiedlichen Namen unterschrieben, in diesem Fall sehen wir „Sabrina".

Warum war das Spear Phishing? Naja, das wurde eben kurz nach Silvester verschickt, und man weiß, dass da viele Leute feiern. Daher haben wir gehofft, dass insbesondere auch Studierende Silvester zusammen mit anderen Menschen feiern und dort eventuell auch Fotos machen. Das war jetzt nicht so super gezielt, aber schon ein bisschen an die Empfänger:innen angepasst.

Wir haben uns auch bemüht, ein bisschen „Jugendsprache" zu sprechen. Das klingt jetzt ein wenig blöd, aber die ganzen Fehler, die Kleinschreibung in der E-Mail usw., das war einfach ein Versuch, sich anzupassen. Und wir hatten diese Nachrichten von Facebook-Accounts und von E-Mail-Accounts geschickt, die alle zu nichtexistierenden Personen gehören. Wir haben bei den Facebook-Accounts sogar variiert, wie viel Inhalte ein Account hat. Da gab es zum Beispiel den Account von einem „Tobias", der irgendwie gar nichts auf seinem Profil hatte, und den Account von einem „Daniel", der ein bisschen mehr hatte, ein paar Infos, und mehr nach einer realen Person aussah.

Ergebnisse

Wir hatten eine ganz gute Klickrate, insbesondere mehr als 40 % bei Facebook und 20 % bei E-Mail. Und da sagen vielleicht einige Leute, das waren dann blöde Studenten, was soll man denn noch von ihnen erwarten. Ich hoffe, dass ich diese Einstellung ein bisschen abmildern kann, wenn ich erzähle, was wir herausgefunden haben. Wie erklären denn die Nutzenden, warum sie geklickt haben? Ich habe dazu ein paar wörtliche Zitate gesammelt (siehe Kasten Seite 34). Was ich fett gekennzeichnet habe, sind Gründe, die man hier bei der Textanalyse herauslesen könnte.

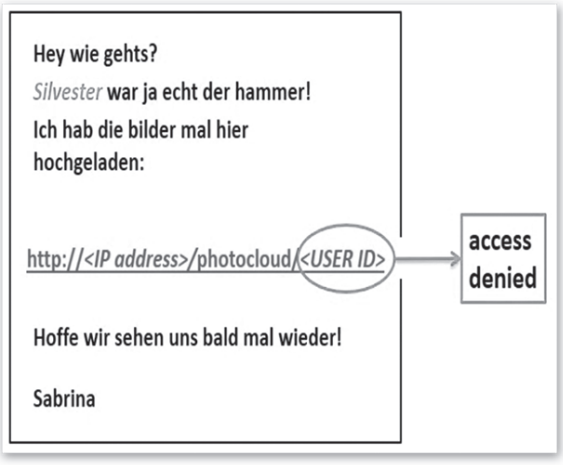


Abbildung 1: Text einer Phishing-Nachricht

Da hat jemand aus Neugier geklickt. Neugier ist eine sehr gute Eigenschaft. Sie führt zum Beispiel dazu, dass man Forschung betreibt oder sich informiert. *Wollte sehen, was passiert.* Das ist auch Neugier, nur anders ausgedrückt. *Ich dachte das ist eine Mail von einem Freund.* Warum dachte die Person das? Naja, wir haben die Top Ten der Vornamen der Studierendengeneration – man weiß ja ungefähr, wie alt sie sind – benutzt, und da gab es wohl ein paar Tobiasse, Daniels und Sabrinas, von denen man etwas erwartet hat oder die man kannte. Dann war jemand an Fotos interessiert, die von Leuten stammen hätten können, mit denen die Person Silvester verbracht hatte. Wir haben dann alles kategorisiert (siehe Tabelle 1).

– 34 %	Neugier/Interesse
– 27 %	Inhalt plausibel, wie erwartet (passt zur eigenen Silvesterfeier)
– 17 %	Nachforschungen (Was ist passiert? Kann ich helfen?)
– 16 %	dachten, dass sie den Absender kennen
– 11 %	Vertrauen in Technologie/Organisation
– 7 %	Angst
– 2 %	automatisch

Tabelle 1: Gründe für das Anklicken der Phishing-Nachricht (Mehrfachnennung möglich)

Am häufigsten haben Leute aus Neugier und Interesse geklickt. Dann haben sie geklickt, weil der Inhalt plausibel schien und in diesem Fall zur eigenen Silvesterfeier passte. Einige Leute haben Nachforschungen angestellt. Sie wussten, es kann nicht für sie sein, aber sie wollten herausfinden, was passiert ist. Vielleicht könnten sie die Nachricht weiterleiten, vielleicht Leute auf den Fotos erkennen. Und relativ viele dachten auch, dass sie den Sender kennen. Da hat es sich gelohnt, diese Top Ten der deutschen Vor- und Nachnamen zu verwenden.

Ein weiterer wichtiger Grund – das ist vielleicht auch für Leute interessant, die in Firmen für IT-Sicherheit verantwortlich sind – ist Vertrauen in Technologie und Organisation. Da haben Leute gesagt, mein Computer oder mein Antivirus-Programm wird mich schützen. Oder, ich habe einen sicheren Browser benutzt, in einem sicheren Betriebssystem wie macOS. Oder, ich bin über Tor gegangen – was natürlich gegen Spear Phishing nicht wirklich hilft. Manche Leute haben gegoogelt, nach dem Link oder nach der E-Mail-Adresse, von der die Nachricht kam. Und es gab auch welche, die gesagt haben, die IP kam aus der Uni Erlangen, also schon technisch versiert. Oder, die Webmail der Uni Erlangen war bisher sicher und ich glaube, da kommt auch kein Spam und nichts Gefährliches rein.

Ein sehr interessanter Grund ist Angst. Die Angst, ob ein Fremder Fotos von mir haben könnte. Es ist durchaus möglich heutzutage, dass mich jemand fotografiert hat und ich das überhaupt nicht bemerkt habe. Und jetzt wer weiß was auf diesen Fotos ist. Das heißt, auch Klicken ist nicht immer ein Zeichen von fehlendem Sicherheitsbewusstsein. Es kann das Ergebnis einer Abwägung sein, zwischen der Angst, eventuell den Rechner zu infizieren, und der Angst, dass die eigenen Fotos in fremden Händen sind.

Wörtliche Zitate von Phishing-Opfern

„Ich wollte mir die Fotos ansehen, aus reiner **Neugier**. Obwohl ich mir dachte, es könnte ein Virus sein – ich habe das Konto daraufhin blockiert."

„Wollte sehen, was passiert …"

„Ich dachte das ist eine **Mail von einem Freund** und war **gespannt** auf die Bilder."

„Weil ich an den Fotos **interessiert** war, und die Nachricht durchaus **von Leuten stammen hätte können,** mit denen ich Silvester verbracht habe."

„Weil ich anhand möglicher Bilder erkennen wollte, **ob ich die Person eventuell kenne.** Da ich **privat gefeiert** habe und nur wenige mir unbekannte Freunde meiner Freunde da waren, habe ich die Gefahr nicht hoch eingestuft. Ebenso wenig Gefahr empfand ich, da ich die **Webmail der Uni bisher für sicher empfand.** Zudem **Interesse** für eventuell lustige Silvesterbilder mir fremder Personen."

„Weil der Link unbedenklich aussah und **mein Computer** bei einem Virusproblem sofort den Zugang verhindert."

„Ich wusste, falls es was gefährliches ist, das **mein Kaspersky** Sicherheitsprogramm mich vor Gefahren schützen wird."

„Da ich mit Firefox einen meiner Meinung nach **sicheren Browser** verwende und zudem **Mac OS** verwende."

„Ich habe den Link in einem anderen **sicheren Browser** geöffnet. (Vorkonfigurierter Firefox aus dem Tor Bundle)"

„Nachdem ich **gegoogelt** habe, schien Photocloud eine sauber Seite zu sein."

„Habe davor die E-Mail Adresse **gegoogelt,** um sicherzugehen, ob etwas über die Adresse im Internet steht"

„**ip kam aus uni erlangen** deshalb dachte ich es kann nix böses sein"

„Ebenso wenig Gefahr empfand ich, da ich die **Webmail der Uni bisher für sicher empfand.**"

„Weil er auf mein Uni-email-konto kam. Hier gab es **noch nie Werbung, Spam, etc**"

„Trotz Unsicherheit war die **Angst** zu groß tatsächlich Bilder von mir in fremden Händen zu wissen, bei heutigem Ausmaß an Möglichkeiten Fotos zu erstellen weiß man schließlich nie wer wo wie unter Umständen doch welche gemacht hat."

„**Aus Reflex,** habe das Fenster aber gleich bevor es geladen hatte wieder geschlossen."

„Ich habe **erst auf den Link geklickt und dann kapiert,** dass eine Person mit diesem Namen eigentlich gar nicht da war"

Am meisten mag ich die Antworten, wo Leute gesagt haben, dass sie aus Reflex geklickt haben. Man klickt einfach zuerst und merkt dann: Moment, was habe ich denn jetzt gemacht? Und natürlich ist die Frage: Könnte es Ihnen passieren? Könnte es mir passieren? Ich weiß nicht, ob es Ihnen passieren kann. Mir kann es passieren, und es ist mir auch passiert. Deswegen bin ich immer sehr vorsichtig, wenn Leute sagen, man muss Awareness schaffen, und Leuten erklären, was passieren kann. Denn ich würde annehmen, dass ich eigentlich Security-aware bin.

Dazu ein erstes persönliches Beispiel. Ich habe erwähnt, dass ich diese Studie auf der Black Hat USA vorgetragen habe, das ist ein ziemlich großes Event – so ein Hackerevent. Und ich habe – das ist so durch die Presse gegangen – sogar von CNN eine E-Mail bekommen. Das ist mir vorher noch nie passiert und danach auch nicht mehr. Und Sie können in Abbildung 2 sehen, das ist ein CNN Request, „Your topic looks fantastic!" und „Here's a link to my work". Und das erste, was ich gemacht habe: Ich habe darauf geklickt. Und als ich dann gesehen habe, wie sich mein Browser öffnet, habe ich mir gedacht: Moment, was habe ich gerade gemacht? Denn alle Informationen, die hier in dieser E-Mail stehen, waren öffentlich zugänglich. Das hätte mir jeder Angreifer problemlos schicken können. Zum Glück war diese E-Mail tatsächlich echt. Aber das zeigt, wie schnell es passiert, dass man sich in einem emotionalen Moment, hier wegen einer E-Mail von CNN, eben verklickt.

From: john.smith@turner.com
To: zinaida.benenson@fau.de
Subject: CNN request -- about your upcoming Black Hat talk
Zinaida,
John at CNN here. I'm the news network's cybersecurity reporter. Here's a link to my work, in case you're not familiar with it.
I saw the description of your upcoming Black Hat talk. Your topic looks fantastic!
Can we get an exclusive look at your research and write the first news story about it?
Cheers,
John Smith
john.smith@CNN.com

Abbildung 2: Echte Anfrage von CNN

Ein anderes Beispiel ist mir vor ungefähr einem Jahr passiert. Wir hatten Kontakt zu einer Firma, die von uns ein Security-Audit haben wollte. Wir haben uns über ein Produkt unterhalten, noch ein Kollege war daran beteiligt, und dann ist das Ganze irgendwie eingeschlafen. Und ein Jahr später, nachdem wir das alles mit der Firma auszuhandeln versucht haben, kam eine E-Mail (Abbildung 3).

From: senior-manager@important-company.com
To: zinaida.benenson@fau.de
Subject: Re: Re: <*Product X*> Security Audit – call follow up

Morning,

Please see attached and confirm.
Any questions please do not hesitate to contact us.

Thanks,
<normal email signature>

Attachment:
Product X_Inquiry.doc

Abbildung 3: Phishing-E-Mail

Das war tatsächlich eine passende Antwort auf eine E-Mail, die ich vorher geschickt hatte. Da steht „Product X" (also das, worüber wir vorher gesprochen hatten) „Security Audit – call follow up", „Please see attached and confirm". Und es war auch ein Dokument beigefügt. Ich war schon dabei, darauf zu klicken, dann ist mir eingefallen: Moment, solche Beispiele erzähle ich doch die ganze Zeit in der Vorlesung, also vielleicht doch lieber nicht klicken. Dann bin ich aus dem Büro gestürmt, ins Büro von meinem Kollegen, der auch an dem Projekt beteiligt war, mit einem Schrei: „Bitte nicht klicken!" Er hat mich so angeschaut von seinem Rechner und meinte: „Ich habe schon geklickt." Ich meinte dann: „Und?" „Ja nichts. Mein Antivirus ist hochgegangen." Das heißt, er hatte Glück, und ich hatte auch Glück, denn es war irgendwas drin, es war tatsächlich ein Angriff, aber zum Glück konnte es durch den Antivirus abgefangen werden. Und das war eine Person, die sich seit fünf Jahren sehr erfolgreich mit IT-Sicherheit professionell beschäftigt hatte.

Was folgt daraus? Ein Kollege und ich, wir wurden beide in einem Moment gefangen, wo wir keinen Verdacht geschöpft haben. Das heißt, eigentlich müssten die Nutzer:innen, wenn sie diese Angriffe abwehren sollen, immer misstrauisch sein; egal, was kommt, egal, ob die Nachricht plausibel ist, egal, ob sie deren Erwartungen entspricht, egal, ob man den Absender kennt. Also muss man sich immer in einem Zustand des permanenten Misstrauens befinden, wenn man tatsächlich 100 % dieser Angriffe abwehren möchte. Und das ist etwas, was man gerne *Sicherheitsmentalität* nennt.

Psychologie der Sicherheitsmentalität

Sehen wir uns doch diese Sicherheitsmentalität mit Hilfe von Psychologie etwas näher an. Ich weiß nicht, ob viele von Ihnen das Buch *Schnelles Denken, langsames Denken* von Daniel Kahneman gelesen haben. Kahneman ist Nobelpreisträger in der Ökonomie, aber eigentlich Psychologe. Er unterscheidet zwischen zwei Systemen des Denkens. System 1 ist die Intuition, aus dem Bauchgefühl handeln. Und System 2 ist logisches Denken. Ich zitiere einfach aus dem Buch, damit Sie vielleicht besser nachvollziehen und mir vielleicht auch glauben können, was ich meine. Es gibt eine „wachsende Zahl von empirischen Befunden, die darauf hindeuten, dass eine positive Stimmungslage, Intuition, Kreativität, Leichtgläubigkeit und zunehmende Beanspruchung von System 1 ein Cluster bilden". Was bedeutet das? Wenn man in System 1 ist, im Flow, in Intuition, in Kreativität, hat man eine positive Stimmungslage, ist aber auch leichtgläubig, und das ist ein Cluster.

Welches Cluster gibt es denn für System 2? „Andererseits sind auch Niedergeschlagenheit, Vigilanz, Argwohn, eine analytische Herangehensweise und vermehrte Anstrengung eng miteinander verbunden." Man kann nicht gleichzeitig leichtgläubig und argwöhnisch sein. Man kann nicht gleichzeitig positive Stimmungslage und Niedergeschlagenheit verspüren. Das heißt, wir können normalerweise nur in einem der beiden Systeme sein. Und weil System 2 mit vermehrter Anstrengung verbunden ist, sind wir normalerweise im System-1-Zustand. Und das ist etwas, was wirklich jeder von uns macht, praktisch fast jede Minute unseres Lebens. Und nur sehr selten schalten wir unser logisches Denken ein, dafür brauchen wir spezielle Trigger, sonst

wäre es eine zu hohe Anstrengung, das würden wir einfach nicht durchhalten.

Wenn wir jetzt sagen, die Mitarbeiter:innen, die Nutzer:innen sollen gezielte Angriffe stets erfolgreich abwehren, dann wollen wir eigentlich, dass sie sich ständig in System 2 befinden – überall – in der Beratung, im Verkauf, in der Presseabteilung, in der Kundenbetreuung, in der Personalabteilung und auch zu Hause. Manche Unternehmen meinen vielleicht, im Beruf sollte es doch möglich sein, unter bestimmten Voraussetzungen in all diesen Abteilungen Leute mit sehr hohem Sicherheitsbewusstsein zu haben. Nur sollte man dann wohl Stellenanzeigen und Gehälter ein bisschen anpassen – und geeignetes Training wäre natürlich auch nötig. Im Privatleben dagegen sieht man sofort, dass das zu kompliziert würde und deswegen auch nicht realistisch ist.

Und dann gibt es noch dieses schöne Problem der False Negatives und False Positives. *False Negatives* heißt hier, dass gefährliche Nachrichten nicht entdeckt werden. Sicherheitsexpert:innen bemühen sich natürlich vorwiegend um diese, denn sie wollen ja die Gefahren abwehren. *False Positives* sind gutartige Nachrichten, die irrtümlich als gefährlich eingestuft werden. Und für die normalen Nutzer:innen ist das total wichtig, denn wenn diese Nachrichten ausgefiltert oder gelöscht oder nicht ernst genommen werden, dann gibt es vielleicht verpasste Chancen oder geschäftliche und persönliche Konflikte.

Und hierzu wieder ein persönliches Beispiel aus meinem Forschungsleben. Ich habe einmal von einer Firma, mit der ich ein Projekt hatte, die Nachricht aus Abbildung 4 bekommen. Aha, „we need your bank account details". Und ich dachte mir: „Hahaha. Ja, das mache ich natürlich. Klar!" Und dann habe ich gemerkt, das scheint ja an mich adressiert zu sein, wenn auch nicht direkt, aber jedenfalls steht mein Name drin. Also habe ich die Firma auf einem separaten Kanal angeschrieben und gefragt:

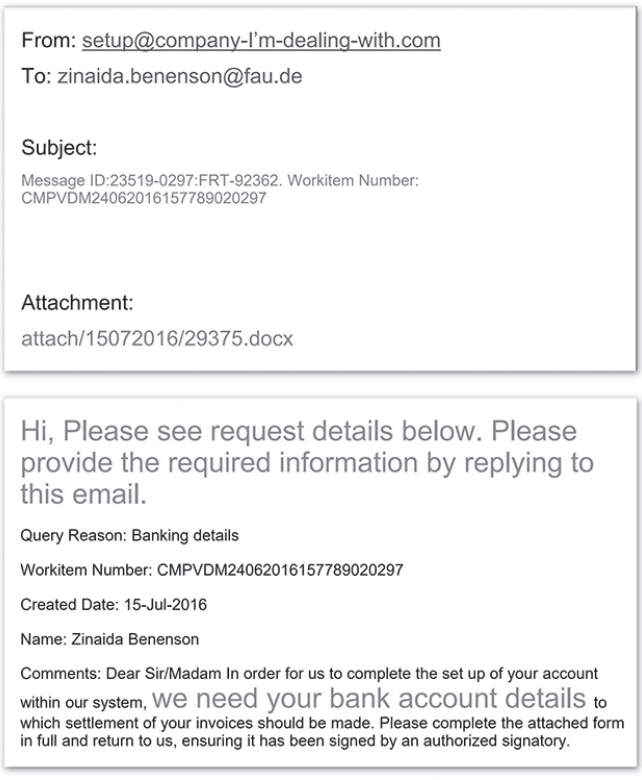


Abbildung 4: Phishing oder echt?

„Habt ihr das geschickt?" Und sie haben geantwortet: „Ja, haben wir. Ist ja nichts Besonderes."

Solche Dinge passieren im Geschäftsleben, denke ich, nicht sehr selten. Und deswegen ist es sehr schwer, da auf der Hut zu sein. Auch private Nutzer:innen bekommen widersprüchliche Awareness-Hinweise. Ich bin PayPal-Kundin und bekomme ab und zu eine PayPal-Kontoübersicht. In dieser legitimen E-Mail gibt es eine Schaltfläche „Weiter zu PayPal", hinter der sich ein Link verbirgt. Dieser Link beginnt aber nicht mit www.paypal.com, wie in den Awareness-Hinweisen von PayPal behauptet. Die Ungenauigkeit der Hinweise führt also zu False Positives.

In den Awareness-Hinweisen von PayPal steht auch, dass eine gefälschte E-Mail meist mit einer unpersönlichen Anrede beginnt. Diese Fehleinschätzung von PayPal kann zu False Negatives führen. Denn in den letzten Jahren haben viele Phishing-E-Mails eine korrekte Anrede benutzt.[3] Der Grund ist, dass persönliche Daten massenweise geleakt wurden. Und natürlich werden von Kriminellen im Darknet oder auf anderen Schwarzmärkten im Internet E-Mail-Adressen, Anreden usw. gehandelt.

Es gab sogar eine Ransomware, die tatsächlich Stellenanzeigen analysiert und gezielte Angriffe an Personalabteilungen verschickt hat, mit Erwähnung von aktuellen Stellenanzeigen.[4] Da fragt man sich, wie man sich denn dagegen schützen soll.

Phishing-as-a-Service?

Aber es gibt Leute, die sagen, wenn wir unsere Nutzer:innen daran gewöhnen, indem wir simulierte Phishing-Angriffe durchführen, dann werden sie vielleicht aware und sich dann doch irgendwie besser verhalten. Und hier habe ich auch ein Beispiel, zum Glück nicht aus meinem persönlichen Leben, aber das ging mal durch die Zeitungen. Das war im Dezember 2015, ich weiß nicht, ob Sie es bemerkt haben. Da wurde an zwei Dienststellen der Berliner Polizei eine E-Mail gesandt, die sie darum gebeten hat, ihre dienstlichen und privaten Passwörter im „sicheren Passwortspeicher der Polizei Berlin (SPS)" zu deponieren. Und dazu gab es einen Link, die E-Mail war im Corporate Design, unterschrieben mit *Zentrale Service Einheit* (ZSE), mit Adressen mit leichten Fehlern, von nichtexistierenden Personen.

Das hat in einer Panik resultiert in den Dienststellen, und deshalb ist das alles in die Presse geraten. Aber eigentlich war es eine simulierte Phishing-Attacke. Das war kein richtiger Angriff. Die Nachricht wurde von einer beauftragten Pentesting-Firma verschickt, von außerhalb der Organisation, und ging an mehr als 400 Leute.

Pentesting the Humans

Mehr als die Hälfte haben geklickt und über 30 Personen haben Nutzerdaten eingegeben, aber wir wissen nicht, was sie da angegeben haben. Ich nenne das – nicht sehr politisch korrekt vielleicht – „Pentesting the Humans". *Pentesting* oder *Penetration Test* ist eine Sicherheitsmaßnahme, die zum Beispiel Firmen verwenden. Wenn sie Software auf Sicherheitslücken überprüfen wollen, lassen sie ihre eigene Software oder ihre eigenen

Netze von sogenannten *Pentestern* hacken. Und hier werden eben Menschen irgendwie gehackt.

Die Polizei musste sich zu dem Ganzen natürlich äußern, weil das in der Presse war. Ein Vorstandsmitglied der Gewerkschaft der Polizei meinte, es würde keine Konsequenzen geben für Leute, die darauf reingefallen sind; die Beamten bekämen „eine Flut von dienstlichen Mails – da schaut man nicht mehr so genau hin". Und resümierte: „Die Polizei ist nur ein Spiegelbild unserer Gesellschaft." Ich finde, das ist sehr weise und sehr richtig gesagt.

Was können wir daraus lernen? Was kann die Polizei daraus lernen? Wir können lernen, dass Polizisten Menschen sind, so wie wir auch. Sie haben auch System 1 und System 2. Und da frage ich mich auch, was denn das richtige Verhalten wäre? Sollen die jede interne E-Mail überprüfen, vielleicht die Person anrufen? Oder schauen, ob die Person existiert, jedes Mal, wenn sie etwas bekommen? Jeder E-Mail misstrauen, die ganze Zeit im System-2-Zustand sein?

Das Netz war da irgendwie voll mit Foren, zum Beispiel bei Heise, voll mit abfälligen Kommentaren über die Polizei, die ich völlig unangebracht finde. Hier ist es wirklich ganz offensichtlich für mich: es waren nicht die Polizisten, die etwas falsch gemacht haben, als sie drauf geklickt haben.

Warum ist Security Awareness schwierig?

Also fragen wir uns, warum ist Security Awareness schwierig? Oder warum behaupte ich, dass Security Awareness schwierig ist? Erstens, Security Awareness heißt, dass man nicht nur aware ist, man muss auch sein Verhalten ändern. Und Verhaltensänderungen sind immer schwierig, das wissen wir alle. Alle, die versucht haben, mehr Sport zu treiben, mehr Gemüse zu essen, rechtzeitig schlafen zu gehen, rechtzeitig ihre Vorträge vorzubereiten usw. und so fort. Ich habe meinen Vortrag diese Nacht vorbereitet, obwohl ich mir schon mehrmals geschworen habe, dass ich es nicht mehr tun werde.

Und Aufrechterhalten des Sicherheitsverhaltens ist schwer. Ständige Wachsamkeit ermüdet, denn es ist ein System-2-Zustand. Man wechselt zwangsläufig in den System-1-Zustand, und dann springen Emotionen und Automatismen an.

Und auch Geschäftsvorfälle und Arbeitspraktiken kollidieren mit Sicherheitsverhalten. Man kann eben nicht bei jeder E-Mail mit Anhängen und Links fragen: Hast du das geschickt? Und bist du sicher, dass es sicher ist? Das wäre schon vom Zeitaufwand schwierig. Und dann stehen natürlich auch unsere sozialen Verhaltensnormen dagegen. Vertrauen und sozialverträgliches Verhalten ist anders. Da fragt man nicht ständig nach. Was also, wenn man sagt: Dein Sicherheitsverhalten muss so und so sein. Dann denken sich normale Nutzer:innen: Was würde passieren, wenn ich zum Beispiel Kolleg:innen oder Vorgesetzte frage, ob sie wirklich diese E-Mail verschickt haben? Sie könnten das für Zeitverschwendung halten. Sie könnten mich für inkompetent halten oder denken, dass ich sie für inkompetent halte oder ihnen nicht vertraue. Das sind alles Dinge, die so ein Verhalten letztendlich nicht erlauben oder nicht wirklich gutheißen.

Der RSA-Breach

Ein anderes Beispiel, das, finde ich, auch gegen Security Awareness spricht, vielleicht haben einige von Ihnen das auch mitbekommen. RSA, das ist eine Sicherheitsfirma, die unter anderem SecurID-Tokens produziert. Ein solches Token kann z. B. für Zwei-Faktor-Authentisierung benutzt werden.

RSA wurde einmal gehackt, mit sehr weitreichenden Folgen.[5] Der Angriff begann mit einer Phishing-E-Mail. Diese E-Mail ging nur an zwei ganz kleine Gruppen von Mitarbeiter:innen. Denn die Kriminellen befürchteten, die Leute in einer Security-Firma würden es sonst merken. Die E-Mail kam von einem *Webmaster* einer Jobbörse und hatte einen Anhang: *Recruitment plan. Please open.* Das haben wir auch in dem Angriff, den ich miterlebt habe, gesehen. Und eine einzige Person in der Personalabteilung hat drauf geklickt. Eine einzige Person.

Was dann passiert ist, möchte ich jetzt nicht genau erklären. Auf jeden Fall sind die Kriminellen von diesem Rechner auf einen anderen Rechner gelangt, und dann weiter ins Netz. Dort haben sie angefangen, Daten zu exfiltrieren. Irgendwann haben Intrusion-Detection-Systeme das gemerkt, Alarm geschlagen und das Ganze wurde dann beendet. Das Problem war allerdings, dass niemand bis heute weiß, was die Kriminellen bis dahin eigentlich gesehen hatten und wo im Netz sie waren. Die Vermutung ist, dass dieses SecurID-Token gehackt wurde, in dem Sinne, dass sie eben mit Hilfe gestohlener Informationen voraussagen konnten, welche Codes so ein Token generieren würde. Und konnten sich damit einloggen.

40 Mio. Tokens ausgetauscht

Es gab natürlich einen großen öffentlichen Aufschrei. Trotzdem war RSA noch glimpflich davongekommen: Der finanzielle Schaden von 70 Mio. US-Dollar war für diese Firma nicht besonders hoch. Auch wurde der Angriff ziemlich schnell bemerkt und RSA konnte sich auch ziemlich gut herausreden. Aber als Folge dieses Hacks wurde wohl der amerikanische Rüstungskonzern Lockheed Martin angegriffen. Die haben aber immer bestritten, dass da irgendwas gestohlen wurde. Wir wissen also eigentlich nicht viel. Trotzdem ist das ein Angriff, über den wir zumindest ein bisschen was wissen. Normalerweise gelangen diese Informationen überhaupt nicht an die Öffentlichkeit. Der Angriff auf RSA erfolgte bereits 2011, wird aber trotzdem häufig als Beispiel benutzt, weil man selten überhaupt etwas Konkretes über einen Angriff auf eine Firma erfährt.[6]

RSA hat Details des Falls veröffentlicht, um transparent zu erscheinen, weil sie natürlich Angst hatten, dass ihnen die Kunden massiv abspringen. Sie mussten vierzig Millionen Tokens austauschen, quasi nur auf Verdacht, dass sie vielleicht gehackt wurden.

Was lernen wir daraus? Gut, RSA ist da irgendwie durchgekommen. Aber natürlich gibt es auch (insbesondere kleine und mittlere) Unternehmen, die diese Mittel nicht haben. Das kann gerade für kleinere Firmen, beispielsweise auch Anwaltskanzleien oder Arztpraxen, tödlich sein. Das sollte man nicht auf die leichte Schulter nehmen.

Und trotzdem ist Awareness eigentlich nicht so wichtig. Es ist schön, wenn Awareness da ist. Aber man kann nicht darauf zählen, dass sie immer ausreicht. Bei RSA hat letztendlich Intrusion Detection und auch schnelles Handeln des Sicherheitspersonals mehr oder weniger zur Begrenzung des Schadens geführt. Was man sich also merken sollte: Awareness-Maßnahmen usw. sind vielleicht gut, um die gröbsten Dinge abzufangen. Aber Angreifer, die es wirklich darauf abgesehen haben, werden reinkommen. Letztendlich müsste man schon darauf vorbereitet sein, die Angriffe zu erkennen und auch zu kommunizieren an alle möglichen Seiten, die involviert sind.

Nutzerzentrierter Schutz

Ich habe ja menschengerechte IT-Sicherheit versprochen. Was könnte man hier tun? Klar ist: unter nutzerzentriert zu verstehen, alle müssen die ganze Zeit aware sein, geht nicht.

Also, was könnte man machen? Angriffe melden. Das soll möglichst schnell geschehen, auch Antworten müssen schnell kommen. Es soll möglich sein, z. B. in einer Firma oder in einer Bank, Paypal von mir aus, Angriffe einfach zu melden. Aber man muss darauf vorbereitet sein, dass viele harmlose Vorkommnisse gemeldet werden. Und dann ist es wieder ein Trade-off. Will ich das überhaupt, als Firma zum Beispiel? Oder nehme ich in Kauf, dass einige Angriffe einfach passieren werden? Ja, das ist auch möglich, das wäre Risikoakzeptanz.

Effektivität und Nutzerfreundlichkeit unbekannt

Verlässliche Indikatoren für das Umschalten in den System-2-Modus müssen da sein. Ein Beispiel für Phishing wäre, externe E-Mails als „extern" zu kennzeichnen. Es gab bis heute keine Studie, die zeigen konnte, ob Effektivität und Nutzerfreundlichkeit dieser Maßnahme irgendwie zufriedenstellend sind. Wir wissen es nicht. Deswegen bin ich da auch vorsichtig. Und letztendlich das Wichtigste ist, Fehler zu erwarten. Also Nutzerfehler werden passieren. Ja, das ist quasi dasselbe wie bei sicherheitskritischen Systemen, die mit Safety zu tun haben. Man muss darauf vorbereitet sein.

Antivirus-Studie

Jetzt stelle ich noch eine zweite Studie vor, über die Nutzbarkeit von Antivirus-Meldungen, die wir auch in meiner Gruppe gemacht haben. Es gab vor einiger Zeit eine Umfrage[7] unter Nutzer:innen und Expert:innen. Auf die Frage „Was sind die drei wichtigsten Dinge, die Sie tun, um sich im Internet zu schützen?" haben etwa 42 % der Nutzer:innen, also der Nicht-Expert:innen, Antivirus genannt. Antivirus scheint also das populärste Tool für diese Gruppe zu sein. Aber was macht Antivirus so toll, haben wir uns gefragt. Denn nur wenige Sicherheitsexpert:innen der Studie, etwa 8 %, nutzen Antivirus. Und man muss sagen, dass Antivirus von Sicherheitsexpert:innen als wirklich total schlecht bewertet wird. „Antivirus is dead", sagt John McAfee[8], „Antivirus is dead and doomed to failure", verschärft Antivirus-Pionier Symantec[9]. „Disable your antivirus software, except Microsoft's", meint ein früherer Mozilla-Ingenieur[10] – da freut sich Microsoft natürlich und titelt: „Antivirus is dead, but Windows Defender is not."[11] Und in welche Richtung die Entwicklung geht, zeigt folgender Rat: „It might be time to stop using antivirus, update your software and OS regularly instead, and practise sceptical computing."[12]

Sceptical computing ist dasselbe wie *constant vigilance.* Aber wir haben bereits gelernt, dass *constant vigilance* nicht das ist, was wir normalen Menschen können. Und das wissen sowohl Expert:innen als auch Nicht-Expert:innen. Dieses *be suspicious of everything* ist in beiden Gruppen eine äußerst unpopuläre Sicherheitsmaßnahme.

Also, was heißt das? Wir gehen zurück zu der Frage: Ist Antivirus dann doch die perfekte Sicherheitsmaßnahme?

Wir haben uns gefragt: Was passiert denn, wenn Antivirus tatsächlich einen Virus entdeckt? Wie reagieren denn Leute darauf? Denn Antivirus ist ja normalerweise irgendwie im Hintergrund, und wenn man da Usability untersuchen möchte, müsste man den irgendwie in den Vordergrund bringen mit irgendeiner Malware. Und wir haben uns gefragt: Verstehen denn die Nutzenden überhaupt Malware-Detection-Nachrichten? Und verstehen sie, dass z. B. eine Datei vom Rechner verschwunden ist, und warum?

Also haben wir uns ein Experiment überlegt. Das haben wir in einem Usability-Labor durchgeführt, wo Leute mit ihrem eigenen Laptop erschienen sind. Wir hatten als Coverstory, dass wir Usability von Word und OpenOffice und so weiter untersuchen. Und wir haben den Teilnehmenden zwei USB-Sticks gegeben mit einer harmlosen Datei, die aber so designed war, dass sie Antivirus aktiviert. Also ein harmloser Virus, könnte man sagen. Beim ersten USB-Stick haben sie die Aufgabe noch ganz normal erledigen können. Aber wenn Sie den zweiten USB-Stick in ihren eigenen Laptop reingesteckt haben, dann gab es zwei Fälle. Entweder wurde eine Datei entfernt, die sie für die Ausführung der Aufgaben nicht brauchen; es handelte sich also um ein *irrelevant infected file.* Oder es wurde eine Datei entfernt, die sie für die Aufgaben brauchen, also ein *relevant infected file.*

So, ich erkläre Ihnen mal ein Beispiel. Wird ein Windows-Rechner durch Windows Defender geschützt, erscheint eine Nachricht vom Windows Defender, verschwindet aber nach drei Sekunden wieder. Der hier betroffene Nutzer hat es nie gemerkt. Was den Nutzer aber genervt hat, war folgende Nachricht vom Windows-Betriebssystem: „An unexpected error is keeping you from copying this file. If you continue to receive this error you can use the error code to search for help." Und dann gibt es den schönen Button „Try again". Den haben die meisten Leute benutzt, ohne dabei überhaupt zu verstehen, was da eigentlich passiert ist. Sie haben ein paar Mal „Try again" geklickt, dann „Skip", und dann war die Datei weg. Und sie haben überhaupt nicht verstanden, warum.

Auf einem anderen Rechner war Avira installiert. Da kommt zuerst eine ähnliche Meldung, die besagt, man braucht Admin-Rechte, um auf die Datei zuzugreifen. Und da kann man fortfahren oder überspringen. Und irgendwann kommt auch die Avira-Meldung. Dieser konkrete Proband hat die Meldung nie bemerkt, weil er so beschäftigt damit war, auf „Vorgang wiederholen" zu klicken.

Was war nun unser Ergebnis mit 40 Leuten, die wir getestet haben? Nur 30 haben überhaupt ihre Augen auf die Antivirus-Nachricht fokussiert, das haben wir mit einem Eye-Tracker festgestellt. 19 haben gemerkt, dass es die Nachricht gab. Ja, das ist ein Unterschied. Manchmal kann man etwas sehen, aber eben nicht im Gehirn verarbeiten. Und 14 haben verstanden, was passiert ist.

Und dann hatten wir 20 Leute, bei denen eine relevante Datei entfernt wurde, und 20, bei denen eine irrelevante Datei entfernt wurde, die sie also nicht brauchten. Aber selbst bei der relevanten Datei haben nicht alle gemerkt, dass sie entfernt wurde. Wie konnte das denn passieren? Nun, sie waren so mit Windows-Fehlermeldungen beschäftigt, dass sie überhaupt nichts mehr gemerkt haben. Und von den Leuten, die diese Datei in dem Moment nicht gebraucht haben, haben es nur neun, also knapp die Hälfte, gemerkt. Und verstanden hat es eigentlich nur ein ganz kleiner Teil der Nutzenden. Von 40 haben nur acht verstanden, was mit der Datei denn eigentlich passiert ist.

Wir haben gelernt, dass die Antivirus-Nachrichten selbst für Windows Defender von Windows-Nachrichten völlig verdeckt werden. Wir haben erkannt, dass die Nachrichten, die rechts unten erscheinen, überhaupt nicht bemerkt werden. Nachrichten in der Mitte des Bildschirms werden bemerkt, aber nicht gelesen und nicht verstanden. Und manche Antivirus-Software fragte die Nutzenden: Was sollen sie denn mit der Datei tun? Das führte zu sehr großer Verunsicherung.

Aber wir haben auch gelernt, dass Antivirus trotzdem, trotz all dieser Probleme, ein ideales Sicherheitsschutztool ist. Warum? Nun, die Nutzenden haben ihrem Antivirus das alles verziehen; haben gesagt, dass sie eigentlich sehr zufrieden sind, insbesondere wenn es nicht kostenlos war, haben gesagt, jetzt sind sie wenigstens sicher, dass es auch funktioniert.

Und die Wahrnehmung ist, ein Antivirus-Tool ist so eine Art Experte und Schutzengel zusammen. Und das macht etwas für mich. Etwas, was ich selber nicht machen kann. Ich kann nicht selber Dateien auf Virus überprüfen. Das kann nur der Antivirus tun. Und das ist sozusagen, trotz diesen Usability-Problemen, etwas, was man anstreben sollte. Dass die Sicherheitsmaßnahmen tatsächlich die Nutzenden schützen und ihnen auch dieses Schutzgefühl vermitteln.

Fazit

Noch einmal zusammengefasst: Was ist nutzerzentrierter Schutz? Erst einmal nutzerzentriertes Denken. Man sollte sich überlegen, welche Auswirkungen der Schutzmaßnahmen es geben könnte: auf Geschäftsvorfälle, Produktivität, normales Leben im Vertrauen, soziale Normen im Arbeitsleben, aber auch im Privatleben. Und das gilt für alles, sowohl für Richtlinien als auch für technische Maßnahmen und Schulungen. Und wenn man Prozesse für die Nutzenden gestalten möchte, z. B. in einer Firma, dann sollte man sich überlegen: Wie sollen Angriffe von ihnen gemeldet werden? Wie werden sie über Angriffe informiert? Was sollen sie im Angriffsfall tun? Und vor allem: Können sie das alles? Das ist das Wichtigste. Und man sollte auch Fehler erwarten und darauf vorbereitet sein.

Anmerkungen und Referenzen

1 *Benenson Z (2016) Exploiting Curiosity and Context; How to Make People Click on a Dangerous Link Despite Their Security Awareness. Vortragsvideo, Black Hat USA, Las Vegas, NV, 3. August 2016. https://www.youtube.com/watch?v=ThOQ63CyQR4*

2 *Benenson Z, Gassmann F, Landwirth R (2017) Unpacking Spear Phishing Susceptibility. In: Targeted Attacks Workshop at Financial Cryptography and Data Security, Springer 2017. https://www.cl.cam.ac.uk/~rja14/shb17/benenson.pdf*

3 *https://www.zdnet.de/88256621/neue-phishing-mails-sprechen-paypal-nutzer-mit-korrekter-anrede-an/*

4 *https://www.heise.de/security/meldung/Goldeneye-Ransomware-greift-gezielt-Personalabteilungen-an-3562281.html*

5 *Greenberg A (2021) The Full Story of the Stunning RSA Hack Can Finally Be Told. Wired, Backchannel, 20. Mai 2021. https://www.wired.com/story/the-full-story-of-the-stunning-rsa-hack-can-finally-be-told*

6 *Im Falle des beschriebenen RSA Breach kamen erst jetzt – 10 Jahre nach dem Angriff – durch einen Wired-Artikel (vgl. Referenz 4) weitere Details an die Öffentlichkeit, da viele RSA-Beschäftigte durch NDAs (Non-Disclosure-Agreements) bisher zum Schweigen verpflichtet waren.*

7 *Ion I, Reeder R, Consolvo S (2015) „… No one can hack my mind": comparing expert and non-expert security practices. In Proceedings of the Eleventh USENIX Conference on Usable Privacy and Security (SOUPS ,15). USENIX Association, USA, S 327–346*

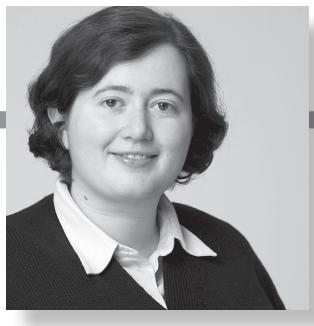
8 *https://thenextweb.com/news/john-mcafee-antivirus-is-dead*

9 *https://www.zdnet.com/article/symantec-calls-antivirus-doomed-as-security-giants-fight-for-survival/*

10 *https://www.bleepingcomputer.com/news/security/former-mozilla-engineer-disable-your-antivirus-software-except-microsofts/*

11 *https://laptrinhx.com/antivirus-is-dead-but-windows-defender-is-not-says-microsoft-3863457969/amp/*

12 *https://arstechnica.com/information-technology/2017/01/antivirus-is-bad/*



Zinaida Benenson

Dr. **Zinaida Benenson** leitet die Forschungsgruppe *Human Factors in Security and Privacy* an der Friedrich-Alexander-Universität Erlangen-Nürnberg. Ihre Forschungsschwerpunkte sind benutzbare IT-Sicherheit, Social-Engineering-Angriffe sowie Sicherheit im Internet der Dinge.

NETZPOLITIK.ORG

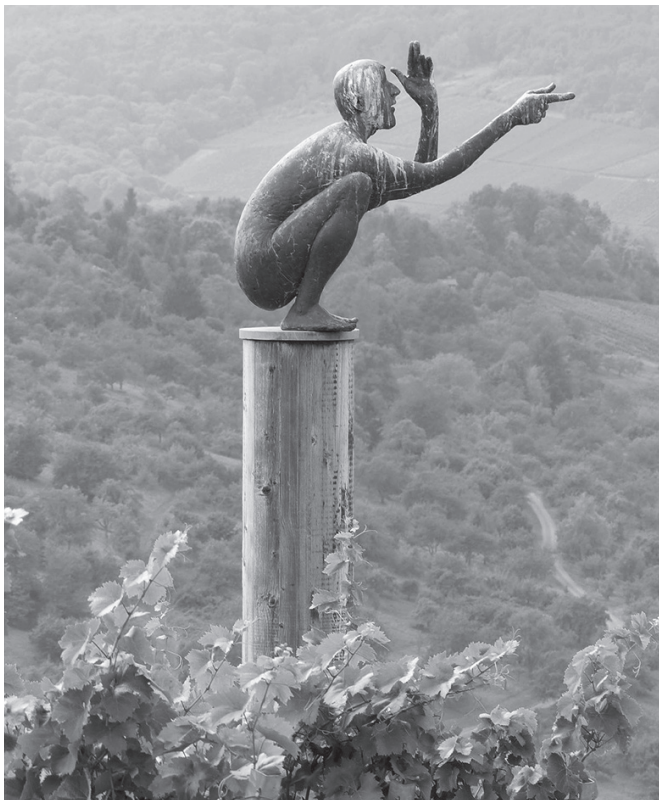
Alexander Fanta

Orbán-Regierung belauschte Journalist:innen

Enthüllungen über die Trojaner-Software Pegasus sorgen in Brüssel für Aufregung, denn eingesetzt wurde sie auch im EU-Land Ungarn. Kommissionschefin von der Leyen bezeichnete das als „komplett inakzeptabel". Abgeordnete fordern von ihr ernsthafte Schritte gegen die Regierung von Viktor Orbán.

Dass die ungarische Regierung offenbar systematisch Journalist:innen und Oppositionelle mit dem Staatstrojaner Pegasus ausspioniert hat, sorgt in Brüssel für Empörung. EU-Kommissionschefin Ursula von der Leyen sagte bei einer Pressekonferenz in Prag[1], wenn sich die Berichte bestätigten, sei eine solche Überwachung „komplett inakzeptabel und geht gegen jegliche Regeln, die wir in der Europäischen Union bezüglich der Pressefreiheit haben". Ob die Kommission deshalb aber Schritte gegen die ungarische Regierung einleitet, konnte ein Kommissionssprecher in Brüssel zunächst nicht sagen.[2]

Am Sonntagabend hatten internationale Medien über eine geleakte Liste mit rund 50.000 Telefonnummern berichtet, die mit Hilfe des Staatstrojaners Pegasus der israelischen Firma NSO Group gehackt und ausspioniert worden sein könnten. Zugespielt wurde die Liste Amnesty International und der Pariser NGO Forbidden Stories, die sie mit 16 Medienorganisationen weltweit teilte. Bei den Zielpersonen im Visier von Pegasus handelt es sich vielfach um Journalist:innen, NGO-Leute und Oppositionelle aus Staaten wie Aserbaidschan, Mexiko, Ruanda, Saudi-Arabien und Indien. Die einzige EU-Regierung, die nach den Recherchen Überwachungsziele auf der Liste beigesteuert hat, ist Ungarn.



„Späher" von Karl-Ulrich Nuss, 1999, Skulpturenpfad in Winterbach-Strümpfelbach – JürgenG, CC BY-SA 3.0

Laut der Recherche finden sich auf der Überwachungsliste aus Ungarn zumindest zehn Anwält:innen, eine Figur aus der Opposition und fünf Journalist:innen, wie der britische Guardian aufzählt.[3] Dazu gehöre auch der bekannte Journalist Szabolcs Panyi von Direkt36, eines der letzten unabhängigen Medien in Ungarn. Nach den Recherchen genehmigte das ungarische Justizministerium in diesem Jahr im Schnitt täglich fünf solcher Überwachungsmaßnahmen für Zwecke der „nationalen Sicherheit".

Warnung vor „schöner neuer Welt der Autokraten"

Die Recherchen zeigten, wie gefährdet Privatsphäre und Pressefreiheit auch in Europa seien, sagte der FDP-Europaabgeordnete Moritz Körner gegenüber netzpolitik.org. Europäische Grundwerte seien in Ungarn unter die Räder gekommen. „Der Fall zeigt außerdem, dass bei weiteren Sicherheitsinstrumenten auf europäischer Ebene wie zum Beispiel E-Evidence mit Blick auf Ungarn große Vorsicht geboten ist." Die E-Evidence-Verordnung soll Behörden in der ganzen EU vereinfacht grenzüberschreitenden Datenzugriff in Ermittlungsverfahren geben. Inwiefern es dabei Schutzmaßnahmen gegen Missbrauch durch Behörden etwa in Ungarn und Polen gibt, ist Gegenstand der laufenden Verhandlungen.[4]

Empört zeigte sich auch der Ko-Fraktionschef der Linken, Martin Schirdewan. Er sprach auf Twitter[5] in Anspielung an den dystopischen Roman von Aldous Huxley von einer „schönen neuen Welt der Autokraten".

Auf Anfrage der Süddeutschen Zeitung betonte die ungarische Regierung, „staatliche Stellen, die befugt sind, verdeckte Methoden einzusetzen" würden „regelmäßig von staatlichen und nicht-staatlichen Institutionen kontrolliert". Stimmen aus der ungarischen Zivilgesellschaft betonen allerdings, es gebe keine effektive, unabhängige Kontrolle der Geheimdienste, schreibt die SZ. Im ungarischen Parlament hat die Regierung von Ministerpräsident Viktor Orbán eine Zweidrittelmehrheit, in der Pandemie entmachtete Orbán zeitweise das Parlament und regierte per Dekret.[6]

Attacken der ungarischen Regierung gegen unabhängige Medien und die Justiz sorgen immer wieder für Kritik der EU-Kommission, Abgeordneten und Mitgliedsstaaten. Seit Jahren läuft ein Rechtstaatlichkeitsverfahren gegen Ungarn und Polen nach Artikel 7 des EU-Vertrages, gegen Sanktionen durch die anderen EU-Länder haben sich die beiden Staaten aber gegenseitig geschützt. EU-Kommissionschefin Ursula von der Leyen hat zuletzt angedroht, EU-Mittel für Ungarn zurückzuhalten[7], wenn das Land nichts gegen seine Defizite bei der Rechtsstaatlichkeit unternehme. Angesprochen auf die Pegasus-Enthüllungen sagte der Kommissionssprecher, die EU-Kommission werde die Sache weiter verfolgen.

Grüne Kritik an „halbherziger" Reaktion von der Leyens

Der Grünen-Abgeordnete Sven Giegold zeigte sich auf Anfrage von netzpolitik.org genervt von der „sehr halbherzigen" Reaktion von der Leyens. Die Überwachung von Nachrichtenmedien biete eine „idealtypische Rechtsbasis für ein Vertragsverletzungsverfahren" gegen Ungarn. Die Forderung der Grünen sei, ein solches Verfahren sofort zu prüfen.

Die EU-Kommission sei aber bereits bislang zu feige gewesen, um Urteile des Europäischen Gerichtshofs in Sanktionen zu übersetzen, kritisiert Giegold. Er verweist auf Urteile des EU-Gerichts gegen das umstrittene ungarische NGO-Gesetz[8], das Hochschulgesetz, mit dem die Central European University aus Budapest vertrieben wurde[9], sowie eine Entscheidung gegen illegale Pushbacks von Schutzsuchenden an der Grenze.[10] Wenn die EU-Kommission solche Fälle nochmal vor den EuGH bringe, könnte dieser hohe Sanktionen etwa in Form von täglichen Geldstrafen gegen Ungarn verhängen, bis die Gesetze zurückgenommen seien. „Das ist die Sprache, die Orbán versteht", sagte Giegold.

Kritik übte der Abgeordnete auch an der deutschen Bundesregierung. Diese verwende Ressourcen auf Staatstrojaner, statt durch das Schließen von Sicherheitslücken für IT-Sicherheit zu sorgen.

SPD-Abgeordneter: „Staatstrojaner verbieten"

Der SPD- Europaabgeordnete Tiemo Wölken bezeichnete „staatlich geduldete Sicherheitslücken in Software" für Journalist:innen und Aktivist:innen als lebensgefährlich[11]: „Die Konsequenz aus den Pegasus-Enthüllungen muss sein, dass Sicherheitslücken sofort gemeldet und Maßnahmen wie Staatstrojaner verboten werden."

Erst vor einigen Wochen hatte der Bundestag mit Stimmen von Union und SPD[12] allen 19 Geheimdiensten erlaubt, Geräte wie Smartphones oder Computer mit Staatstrojanern zu hacken. Angesichts der Enthüllungen zu Pegasus hat netzpolitik.org beim Bundeskriminalamt[13] nach Unterlagen zu einem möglichen Einsatz des umstrittenen Staatstrojaners in Deutschland angefragt.

Quelle: https://netzpolitik.org/2021/staatstrojaner-pegasus-orban-regierung-belauschte-journalistinnen/

Anmerkungen

1 *https://audiovisual.ec.europa.eu/en/video/I-209503*
2 *https://audiovisual.ec.europa.eu/en/video/I-209203*
3 *https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests*
4 *https://netzpolitik.org/2020/eevidence-parlament-will-etwas-mehr-schutz-bei-behoerdlichen-datenzugriffen-in-drittstaaten/*
5 *https://twitter.com/schirdewan/status/1416811019138211843?s=20*
6 *https://www.zeit.de/politik/ausland/2020-03/ungarn-viktor-orban-notstandsgesetz-ermaechtigungsgesetz-coronavirus*
7 *https://www.faz.net/aktuell/politik/ausland/wie-von-der-leyen-ungarn-zum-einlenken-zwingen-will-17426333.html*
8 *https://www.zeit.de/politik/ausland/2020-06/eugh-urteil-ngo-gesetz-ungarn-eu-recht*
9 *https://www.faz.net/aktuell/politik/ausland/eugh-urteil-ungarns-hochschulgesetz-verstoesst-gegen-eu-recht-16988304.html*
10 *https://www.derstandard.at/story/2000122599161/ungarn-kassierte-bei-asylrecht-niederlage-vor-dem-eugh*
11 *https://twitter.com/woelken/status/1417099164404666369*
12 *https://netzpolitik.org/2021/verfassungsschutz-und-bundespolizei-bundestag-beschliesst-staatstrojaner-fuer-geheimdienste-und-vor-straftaten/*
13 *https://fragdenstaat.de/anfrage/nso-pegagus/*
14 *https://www.otto-brenner-stiftung.de/wissenschaftsportal/informationsseiten-zu-studien/medienmaezen-google/*
15 *http://pool.sks-keyservers.net/pks/lookup?op=get&search=0x2271FE6D4CD84C62*

Alexander Fanta

Alexander Fanta berichtet als Brüssel-Korrespondent von *netzpolitik.org* über die Digitalpolitik der Europäischen Union. Er schreibt über neue Gesetze und recherchiert investigativ über große Technologiekonzerne und ihr Lobbying. Er ist Ko-Autor der Studie *Medienmäzen Google*[14] über Journalismusförderungen des Konzerns. 2017 war Alexander Stipendiat am Reuters-Institut für Journalismusforschung an der Universität Oxford, wo er zur Automatisierung im Journalismus forschte. Davor war er Außenpolitikjournalist bei der österreichischen Nachrichtenagentur APA.
E-Mail: *alexander.fanta@netzpolitik.org* (PGP[15]). Twitter: *@FantaAlexx*. WhatsApp/Threema: *+32483248596*.

Tomas Rudl

Wenn digitale Gewalt zu physischer Gewalt wird

In einer groß angelegten Untersuchung zeigt die Organisation Forensic Architecture*, wie verbreitet die Spähsoftware* Pegasus *ist. Die NSO Group liefert sie an Regierungen in aller Welt, die damit Menschenrechtsaktivist:innen, Oppositionelle und Journalist:innen überwachen.*

Die Spyware Pegasus kommt selten allein. Ins Visier der Überwachungssoftware gerät oft nicht nur die eigentliche Zielperson, sondern auch das soziale Umfeld des Opfers. Und oft genug schlägt die digitale Gewalt in physische um: Etwa im Fall des saudi-arabischen Journalisten Jamal Khashoggi, der im Exil überwacht, verfolgt und schließlich ermordet[1] wurde.

Der israelische Softwarehersteller NSO Group und sein Spitzel-Tool Pegasus stehen im Zentrum einer umfangreichen Untersuchung der Menschenrechtsorganisation Forensic Architecture.[2] Mit Hilfe von Amnesty International und dem kanadischen Citizen Lab hat die NGO 15 Monate lang öffentlich verfügbare Informationen ausgewertet, rechtliche Dokumente durchgeackert und mit Dissident:innen, Journalist:innen und Aktivist:innen gesprochen.

Daraus ist die bislang umfassendste Dokumentation der NSO Group und ihrer weltweiten Aktivitäten entstanden. Eine Online-Datenbank visualisiert Fälle[3] aus aller Welt, darunter in Spanien, Mexiko, Saudi Arabien, Indien und Ruanda. Die Filmemacherin Laura Poitras hat Interviews mit Betroffenen geführt, der NSA-Whistleblower Edward Snowden leiht dem Projekt seine Erzählstimme.

Weltweites Überwachungsnetzwerk

Die 2010 gegründete NSO Group gilt als einer der weltweit führenden Hersteller von Überwachungssoftware. Ihr Schlüsselprodukt Pegasus verkauft sie an Nationalstaaten, die damit die Rechner und Mobiltelefone von Verdächtigten hacken und überwachen. Doch anstatt damit Kriminelle oder Terroristen zu jagen, wie es in der Produktbeschreibung steht, findet sich die invasive Software regelmäßig auf Geräten von Menschenrechtsaktivist:innen[4], Oppositionellen[5] und Journalist:innen[6] wieder.

„Es ist eine Schadsoftware, die deine Kamera aktiviert, dein Mikrophon, alles, was ein integraler Teil deines Lebes ist“, berichtet die mexikanische Journalistin Carmen Aristegui in einem der Fallbeispiele.[7] Eine unscheinbar wirkende Textnachricht infizierte Anfang 2015 ihr Handy, die Überwachung weitete sich später auf ihre Kolleg:innen und sogar ihren minderjährigen Sohn aus.

Pegasus von Christian Friedrich Tieck auf dem Westgiebel des Schauspielhauses in Berlin-Mitte – Foto: Ajepbah, CC-BY-SA-3.0 DE

Hintergrund dürften kurz zuvor veröffentlichte investigative Recherchen über den damaligen Präsidenten Enrique Peña Nieto gewesen sein, dem Korruption nachgesagt wurde.

Vor Landesgrenzen machen die Tools der NSO Group nicht halt. Der saudische Dissident Omar Abdulaziz, ein Freund des später ermordeten Jamal Khashoggi, wurde im kanadischen Exil gehackt. Zwei seiner Brüder wurden kurz danach in Saudi Arabien verhaftet. Im Ausland lebende Oppositionelle aus Ruanda erhielten mysteriöse Nachrichten und Anrufe über WhatsApp[8], mit denen sie zunächst unbemerkt gehackt und überwacht wurden.

Moratorium für Spähsoftware gefordert

Die für den Einbruch genutzte Sicherheitslücke hat WhatsApp[9] längst geschlossen, die Mutter Facebook geht inzwischen juristisch gegen NSO Group[10] vor. Doch das Problem bleibt: Die Tools der Überwachungsindustrie gelangen allzu leicht in die falschen Hände[11], unter den Opfern können sich selbst Multi-Milliardäre wie der Amazon-Gründer Jeff Bezos[12] wiederfinden.

Expert:innen fordern schon seit langem eine rigorose Kontrolle des Sektors sowie ein Moratorium für den Verkauf von Spähtechnologie[13], bis eine globale Regulierung gefunden worden ist.

Tomas Rudl

Tomas Rudl ist in Wien aufgewachsen, hat dort für diverse Provider gearbeitet und daneben Politikwissenschaft studiert. Seine journalistische Ausbildung erhielt er im Heise-Verlag, wo er für die Mac & i, c't und Heise Online schrieb. Er ist unter ☎ +49 30 577148268 ✉ oder *tomas@netzpolitik.org* (PGP-Key[20]) erreichbar und twittert mal mehr, mal weniger unter *@tomas_np*

Die lässt jedoch auf sich warten. Zuletzt hatte sich etwa die EU auf bloß zahnlose Exportkontrollen für Spähsoftware[14] geeinigt, ein international abgestimmtes Vorgehen scheint derzeit in weiter Ferne. Firmen wie NSO Group können weiterhin in einem Graubereich operieren: Ein aktueller Bericht von Amnesty International[15] legt nahe, dass das Unternehmen ein schwer durchschaubares Firmengeflecht[16] dazu nutze, etwaige Exportbeschränkungen zu umgehen.

„Die Untersuchung zeigt das Ausmaß, in dem die digitale Sphäre, in der wir leben, die neue Grenze für Menschenrechtsverletzungen geworden ist", sagt Shourideh Molavi, leitende Forscherin für Forensic Architecture. Es handle sich um einen Bereich von staatlicher Überwachung und Einschüchterung, der physische Gewalt in der realen Welt ermögliche, so Molavi.

Auftakt für interdisziplinäre Praxis

In diese Welt schwappt auch die multimediale Untersuchung: Bis zum 8. August läuft die Ausstellung „Investigative Commons" im Haus der Kulturen der Welt[17] in Berlin. Sie präsentiert neue Formen kollaborativer Wahrheitsfindung und investigativer Ästhetik, heißt es in der Beschreibung: Ähnlich der NSO-Untersuchung sollen dabei Open-Source-Ermittlungen mit strategischer, juristischer Menschenrechtsarbeit verknüpft werden, hinzu kommen Methoden von Investigativ-Reporter:innen, Aktivist:innen und Wissenschaftler:innen.

Es soll der Auftakt sein für eine interdisziplinäre Praxis[18], die Forensic Architecture mit dem European Center for Constitutional and Human Rights (ECCHR) angestoßen hat. Gemeinsam mit anderen Gruppen, darunter die investigative Rechercheplattform Bellingcat und die Berliner Initiative Mnemonic, will das breit aufgestellte Netzwerk Verletzungen von Menschenrechten aufdecken.[19]

Quelle: https://netzpolitik.org/2021/spyware-pegasus-wenn-digitale-gewalt-zu-physischer-gewalt-wird/

Anmerkungen

1 *https://netzpolitik.org/2018/troll-armeen-und-spione-der-online-feldzug-der-saudi-arabischen-regierung/*
2 *https://forensic-architecture.org/investigation/digital-violence-how-the-nso-group-enables-state-terror/*
3 *https://www.digitalviolence.org/#/explore*
4 *https://netzpolitik.org/2018/spionagesoftware-pegasus-gegen-amnesty-international-eingesetzt/*
5 *https://netzpolitik.org/2020/wie-autoritaere-staaten-dissidenten-im-ausland-verfolgen/*
6 *https://netzpolitik.org/2020/citizen-lab-dutzende-iphones-von-journalistinnen-gehackt/*
7 *https://www.digitalviolence.org/#/pegasus-stories*
8 *https://www.bbc.com/news/technology-50249859*
9 *https://techcrunch.com/2019/05/13/whatsapp-exploit-let-attackers-install-government-grade-spyware-on-phones/*
10 *https://www.theguardian.com/technology/2020/jul/17/us-judge-whatsapp-lawsuit-against-israeli-spyware-firm-nso-can-proceed*
11 *https://www.zeit.de/digital/datenschutz/2020-12/ueberwachungssoftware-mexiko-rcs-hackingteam-drogenkartell-puebla/komplettansicht*
12 *https://netzpolitik.org/2020/ueberwachungssoftware-saudischer-kronprinz-soll-jeff-bezos-mit-whatsapp-nachricht-gehackt-haben/*
13 *https://netzpolitik.org/2019/un-bericht-fordert-transparentere-zusammenarbeit-zwischen-ueberwachungsunternehmen-und-staaten/*
14 *https://netzpolitik.org/2020/dual-use-verordnung-eu-verwaessert-neue-regeln-fuer-ueberwachungsexporte/*
15 *https://www.amnesty.org/download/Documents/DOC1041822021ENGLISH.PDF*
16 *https://www.digitalviolence.org/#/corporate*
17 *https://www.hkw.de/de/programm/projekte/2021/investigative_commons/start.php*
18 *https://www.sueddeutsche.de/kultur/berlin-haus-der-kulturen-der-welt-ausstellung-investigative-commons-menschenrechte-1.5341956*
19 *https://www.theguardian.com/law/2021/jun/27/berlins-no-1-digital-detective-agency-is-on-the-trail-of-human-rights-abusers*
20 *https://keys.openpgp.org/vks/v1/by-fingerprint/CA052285DC96CFC89E980514745121858AE13AED*

Constanze Kurz

Die Branche der Staatshacker ächten

Wieder wurde der Spionage- und Hackingdienstleister NSO Group beim systematischen Missbrauch seiner Software Pegasus erwischt. Solche Unternehmen gehören geächtet und als das benannt, was sie sind: eine Gefahr für Leib und Leben von Menschen. Ein Kommentar.

Diesmal wird wohl auch keine neue PR-Initiative mit Home-Stories und mit vorher noch nie gewährten Einblicken in die angeblich so wichtige Arbeit gegen das Verbrechen[1] helfen: Dem Spionage- und Hackingdienstleister NSO Group, der die Software namens Pegasus an dutzende Länder verkauft hat, wurde erneut systematischer Missbrauch seiner Technologie nachgewiesen.

Ganze Scharen von Menschenrechtlern, Reportern, Anwälten und politischen Entscheidungsträgern wurden und werden mit der Software ausspioniert oder finden sich auf langen Listen anvisierter Überwachungsopfer. Die an Amnesty International geleakten Listen von Kunden der NSO Group beinhalten über fünfzigtausend Telefonnummern.

Nachzulesen ist das beim am Sonntag an die Öffentlichkeit gegangenen Pegasus-Projekt[2], in dem eine Gruppe von Journalisten gemeinsam ihre Recherchen zur NSO Group und deren Kunden koordiniert hat. Die am Markt der Staatstrojaner- und Spionagesoftware wohlbekannte Firma bezeichnet sich selbst als Führer im Feld des Cyber Warfare[3] und verkauft ihre Überwachungstechnologie weltweit exklusiv an staatliche Behörden.

Das Projekt trägt den Namen der Software Pegasus, die von der NSO Group angeboten wird und iPhones und Android-Telefone ausspionieren kann. Typischerweise werden nach der Infektion heimlich Daten aus Messengern, E-Mail-Programmen oder Foto-Apps ausgeleitet. Aber nicht selten werden auch aktive Hacks durchgeführt, bei denen Mikrofone und Kameras aktiviert oder Ortsdaten in Echtzeit übertragen werden. Praktisch wird das infizierte Telefon zu einer Wanze, die mit dem Gerät durchgeführte, aber auch in der Nähe stattfindende Kommunikation ausspionieren kann.

Rücksichtslose Branche

Damit kommt nicht nur die Privatsphäre der Opfer und deren Kommunikationspartner in den Fokus, sondern auch ihr höchstpersönlicher Bereich, die Intimsphäre. Denn was man neben dem Smartphone so sagt und macht, ist bei vielen Menschen nochmal eine andere Dimension als das, was man ins Gerät hineinspricht oder -tippt. Dafür finden sich in der aktuellen Berichterstattung des Pegasus-Projekts auch prompt wieder konkrete Beispiele: Denn nicht jeder legt sein Telefon in einen anderen Raum, wenn er Sex hat.

Wollen wir wirklich weiterhin dulden, dass man bei jedem Gespräch immer darüber nachdenken müsste, ob das Telefon gerade in Reichweite ist? Wollen wir dulden, dass wir manchmal mit schalem Blick auf das Gerät schauen und denken, ob es wohl doch eine Wanze sein könnte? Und wollen wir diese ganze rücksichtslose Branche weiter mit Steuergeldern alimentieren?

Denn das haben die Parteien CDU, CSU und SPD im Bundestag kürzlich beschlossen[4], als sie das staatliche Hacken und Staatstrojaner auch noch für alle deutschen Geheimdienste erlaubt haben. Künftig werden also auch deutsche Gelder in diesem widerwärtigen Geschäftsfeld landen, denn ohne technische Hilfe aus dieser Branche sehen deutsche Staatshacker alt aus.

Mobiltelefone im Zentrum der Überwachung

Es ist beileibe nicht das erste Mal, dass der israelische Anbieter NSO Group und auch konkret seine Spitzel-Software Pegasus in der öffentlichen Kritik stehen. Erst vor wenigen Tagen machte eine umfangreiche Untersuchung der Menschenrechtsorganisation Forensic Architecture[5] nochmal klar, wie stark Journalisten, Oppositionelle und Aktivisten betroffen sind. Und es ist auch kein Skandal anderer Länder, wenn das deutsche Bundeskriminalamt[6] mitmischt und der bayerische Innenminister sich die Software vorführen lässt.

Dass Mobiltelefone heute im Zentrum der Überwachung stehen, kommt nicht von ungefähr: Für staatliche Behörden ist es mittlerweile ein Leichtes, an SIM-Karten-Daten mit gesicherter Identifizierung zu kommen, übrigens sowohl in demokratischen als auch diktatorischen Staaten. Denn die Zwangsregistrierung mit Identitätsnachweis ist im letzten Jahrzehnt fast überall eingeführt worden. Die Begründung war auch hier die Kriminalitätsbekämpfung. Einmal mehr zeigt sich die Schattenseite dieser einseitigen Politik: Es ist eben auch ein ungeheurer Machtzuwachs für jene, die auf die Telefon-Identifizierungsdaten sämtlicher Menschen zugreifen können.

Was man nach den neuesten Veröffentlichungen, aber im Grunde schon über die seit Jahren anhaltende kritische Berichterstattung festhalten muss, ist die Tatsache, dass um Journalisten, Anwälte oder Aktivisten eben längst kein Bogen mehr gemacht wird, wenn es um das Hacking ihrer Geräte geht – im Gegenteil, sie sind in zunehmendem Maße Ziel. Wenn weiterhin auch in Deutschland jeder Mensch verpflichtet wird, die SIM-Karte des eigenen Telefons mitsamt Identifizierung seiner Person registrieren zu lassen, bedeutet das schlicht, dass sie weiterhin auch Zielscheibe sein können.

Dass es Schadsoftware von Firmen wie der NSO Group auch künftig geben wird, können wir nicht kurzfristig ändern. Auch dass es an lange geforderten effektiven Kontrollen solcher Unternehmen fehlt, kann man vorerst nur weiterhin beklagen. Wir müssen hierzulande als Sofortmaßnahme aber die Identifizierung des eigenen Telefons und der SIM-Karte abschaffen. Denn das schafft die Grundlage dafür, dass der Raum eingeengt ist, in dem noch sicher und unbeobachtet kommuniziert werden kann.

Wer für die Exploits bezahlt

Die NSO Group ist mit einer anwachsenden Liste von Missbrauchsfällen schon über Jahre hinweg unangenehm aufgefallen. Kritik ließ sie stets abtropfen. Damit, dass Spionage-

Unternehmen und auch andere Marktteilnehmer nun ihr Geschäftsgebaren ändern, ist leider nicht zu rechnen. Sie werden weitermachen, finanziert von den Steuerzahlern der Käuferländer und protegiert von deren Regierungen. Die NSO Group dürfte auch weiterhin sogenannte Zero-Day-Exploits nutzen[7], also noch unbekannte Sicherheitslücken, die für hohe Preise gehandelt werden.

All das finanzieren die Kunden solcher Anbieter mit. Allein die US-amerikanischen Behörden geben Millionen Dollar[8] aus, um iPhones und Android-Telefone zu hacken, auch mit Hilfe der NSO Group[9]. Auch Deutschland hat dafür erst kürzlich die Weichen gestellt, indem die Erlaubnis zum staatlichen Hacken gesetzlich noch weiter ausgedehnt wurde.

Der aktuelle Skandal beweist, wie falsch diese Weichenstellung war und wie blind die politischen Entscheider für die Realitäten einer Branche von Staatshackern sind, die sich ihr gutgehendes Geschäft nicht durch Menschenrechte oder durch den Schutz von Geheimnisträgern vermasseln lassen.

Wir alle sind es, die nicht nur direkt, sondern vor allem indirekt dafür bezahlen, dass solche Firmen wie die NSO Group überhaupt legal existieren dürfen. Wir bezahlen mit unsicheren und ausspionierbaren Smartphones, deren Sicherheitslücken aufgekauft statt geschlossen werden. Wir bezahlen aber auch, weil wir hinnehmen, dass Menschen aus dem aktivistischen und journalistischen Bereich mitsamt ihren Familien und ihrem Umfeld nur in Angst noch ihrem Beruf oder ihrer Berufung nachgehen können.

Ich sehe das schon lange nicht mehr ein. Wir brauchen schnellstens eine Ächtung solcher Unternehmen in Deutschland, am liebsten gleich in ganz Europa. Wir müssen sie als das benennen, was sie sind: eine Gefahr für Leib und Leben von Menschen, mit denen man nichts zu schaffen haben darf. Keine deutsche oder europäische Behörde darf je (wieder) Kunde der NSO Group sein.

Quelle: https://netzpolitik.org/2021/schadsoftware-pegasus-die-branche-der-staatshacker-aechten/

Anmerkungen

1 *https://www.technologyreview.com/2020/08/19/1007337/shalev-hulio-nso-group-spyware-interview/*
2 *https://www.zeit.de/politik/ausland/2021-07/spionage-software-pegasus-cyberwaffe-ueberwachung-menschenrechte-enthuellung*
3 *https://www.documentcloud.org/documents/815991-1276-nso-group-brochure-pegasus.html*
4 *https://netzpolitik.org/2021/verfassungsschutz-und-bundespolizei-bundestag-beschliesst-staatstrojaner-fuer-geheimdienste-und-vorstraftaten/*
5 *https://netzpolitik.org/2021/spyware-pegasus-wenn-digitale-gewalt-zu-physischer-gewalt-wird/*
6 *https://www.zeit.de/politik/ausland/2021-07/ueberwachungsaffaere-spionage-software-pegasus-einsatz-deutschland-bundeskriminalamt-handydaten-rechtsstaat*
7 *https://citizenlab.ca/2017/06/reckless-exploit-mexico-nso/*
8 *https://www.forbes.com/sites/thomasbrewster/2017/04/13/post-trump-order-us-immigration-goes-on-mobile-hacking-spending-spree/*
9 *https://www.vice.com/en/article/gygxk9/the-dea-met-with-controversial-iphone-hackers-nso-group*

Infos zur Autorin siehe Seite 57

Tom Jennissen

Uploadfilter werden Gesetz

Mit dem Urheberrechts-Diensteanbietergesetz werden erstmals Uploadfilter gesetzlich vorgeschrieben. Nach diesem Dammbruch ist zu befürchten, dass Uploadfilter künftig nicht nur zur automatisierten Durchsetzung des Urheberrechts zum Einsatz kommen, sondern zum universalen Regulierungswerkzeug werden.

Wenn der Bundestag am heutigen Donnerstag[1] abschließend über die Umsetzung der EU-Urheberrechtsrichtlinie[2] in deutsches Recht abstimmt, werden die im umstrittenen Artikel 17[3] vorgesehenen Uploadfilter endgültig in deutsches Recht gegossen. Größere Diensteanbieter wie etwa YouTube müssen dann nach den Vorgaben des Urheberrechts-Diensteanbietergesetzes (UrhDaG) spätestens ab August sämtliche Inhalte, die hochgeladen werden, automatisiert überprüfen und gegebenenfalls blockieren.

Ein seit Jahrzehnten etablierter Konsens der Internetregulierung ist damit aufgekündigt: Während Plattformen bisher in Notice-and-Takedown-Verfahren auf Hinweise hin vermeintlich rechtswidrige Inhalte prüfen und eventuell löschen mussten, sollen sie nun sämtliche Uploads ihrer Nutzerinnen und Nutzer aktiv überwachen.

Dabei galt es lange in der deutschen Politik als Konsens, dass Inhalte und Nutzende nicht umfassend überwacht werden sollen. Alle im Bundestag vertretenen Parteien haben sich gegen Uploadfilter ausgesprochen und auch die Regierungskoalition hat in ihrem Koalitionsvertrag[4] vom März 2018 unmissverständlich klargemacht: „Eine Verpflichtung von Plattformen zum Einsatz von Upload-Filtern, um von Nutzern hochgeladene Inhalte nach urheberrechtsverletzenden Inhalten zu ‚filtern', lehnen wir als unverhältnismäßig ab."

Dass dieses Versprechen nicht viel Wert war, wurde ziemlich genau ein Jahr später klar, als die Regierung im Rat der Europäischen Union der Urheberrechts-Reform und damit der Einführung von Uploadfiltern zustimmte.

Protest gab es vor allem für strengere Uploadfilter

Verglichen mit den lautstarken Protesten gegen die Einführung des Artikel 17 aus der EU-Richtlinie, bei der hunderttausende meist junge Menschen auf die Straße gingen[5], erfolgte die Umsetzung in nationales Recht vergleichsweise still und ohne eine größere gesellschaftliche Debatte.

Öffentlichkeitswirksamer Protest regte sich vor allem für noch strengere Uploadfilter: Zum Abschluss einer intensiven Kampagne der Rechteindustrie wettern, angeführt von Peter Maffay[6], verschiedene Musikschaffende von Helene Fischer bis SLIME gegen „vermeintlichen Verbraucherschutz" und „Netzaktivist*innen", die aus „ihrem ideologischen Elfenbeinturm heraus […] realitätsferne Zensurszenarien" spinnen würden[7].

Dass sie dabei eine äußerst fragwürdiges Verständnis der Rechtslage[8] kolportieren, mag vielen der Beteiligten nicht bewusst sein. Unmissverständlich ist, dass hier Eigentumsrechte gegen Meinungsfreiheit und Kritik an Überwachung im Netz ausgespielt werden sollen.

Während die Leitlinien der Kommission zur Umsetzung von Artikel 17 weiter auf sich warten lassen[9] und wohl erst nach der offiziellen Umsetzungsfrist im Juni 2021 vorliegen werden, hat der Bundestag Ende März in erster Lesung über den Regierungsentwurf diskutiert. Am 12. April hat die Sachverständigenanhörung im zuständigen Rechtsausschuss[10] stattgefunden, am 18. Mai stimmte der Rechtsausschuss letzten Änderungsanträgen der Koalitionsfraktionen zu.

Dabei kamen die Abgeordneten den Sportverbänden noch weiter entgegen[11] und verschärften die Regeln für Ausschnitte aus Live-Übertragungen. Gleichzeitig stellen die Änderungen klar, dass etwa Karikaturen und Parodien ohne Beschränkungen erlaubt sein sollen und Zitate vergütungsfrei bleiben. Der Beschwerdemechanismus wurde ein wenig verbessert, indem ein struktureller Anreiz zum Overblocking entschärft wurde.

Viele Kritikerinnen und Kritiker von Uploadfiltern haben versucht, sich konstruktiv in den Gesetzgebungsprozess einzubringen. Denn die ersten Vorschläge aus dem Bundesjustizministerium waren erkennbar bemüht, die negativen Auswirkungen von Uploadfiltern abzumildern. Zugleich war abzusehen, dass die Rechteindustrie ihre gesamte Lobbymacht in die Waagschale werfen und versuchen würde, die Uploadfilter möglichst strikt zu gestalten.

Und so kam es denn auch: Nach dem ersten Referentenentwurf sollten Bagatellnutzungen in Grenzen generell erlaubt werden. Nutzende sollten darüber hinaus Uploads als erlaubte Nutzungen kennzeichnen können, wenn es sich etwa um Zitate, Parodien oder Pastiches handelt. Eine solche Kennzeichnungsmöglichkeit sollte es auch beim Bestehen individueller Lizenzen oder für die Verwendung gemeinfreier Werke geben, die der Filter nicht erkennen kann – etwa weil er nicht zwischen verschiedenen Aufnahmen klassischer Musikwerke unterscheiden kann.

Vor allem auf den massiven Druck der Rechteindustrie hin wurden diese Beschränkungen immer weiter aufgeweicht. Die Erlaubnis zur Bagatellnutzung wurde durch ein kompliziertes prozessuales System ersetzt: Statt einer klaren Erlaubnis bestimmter Nutzungen ist nunmehr vorgesehen, dass bei geringfügigen Nutzungen vermutet wird, dass es sich dabei um gesetzlich erlaubte Nutzungen handelt, etwa da sie als Zitat oder zum Zweck der Parodie verwendet werden. Zugleich wurden die Kennzeichnungsmöglichkeiten durch Nutzende stark eingeschränkt und die Bagatellgrenzen sehr eng gezogen. Für Text etwa sind das 160 Zeichen, also weniger als ein Tweet. Und schließlich haben die Rechteinhaber einen „roten Knopf" bekommen, mit dem sie in besonders dringlichen Fällen sofort die Sperrung eines Inhalts bis zur Entscheidung auslösen können. Ein entsprechender „grüner Knopf" für im Sinne der Meinungsbildung dringliche Inhalte ist nicht vorgesehen.

Der Kern des Gesetzes geriet aus dem Blick

Die Zivilgesellschaft, die noch vor zwei Jahren in fundamentaler Opposition auf der Straße stand, fand sich plötzlich in der Rolle, einen Gesetzentwurf, der die umfassende Einführung von Uploadfiltern vorsieht, gegen die Angriffe der Rechteindustrie zu verteidigen, um ein noch schlimmeres Gesetz zu verhindern.

Dabei geriet jedoch der Kern des Gesetzes aus dem Blick: eine umfassende Überwachung sämtlicher User-Uploads durch automatisierte Uploadfilter. Erstmals wird eine automatisierte Infrastruktur gesetzlich vorgeschrieben, die sämtliche User-Uploads auf größeren Plattformen durchsucht. Und selbst wenn nicht alle Inhalte in diesem Filter hängen bleiben und die Hoffnung besteht, dass Memes und Remixe zumindest in Grenzen online gehen können: Durchleuchtet und überprüft – also überwacht – werden die Inhalte dennoch.

Uploadfilter könnten sich in der Regulierung des Internets als der Hammer erweisen, der alle Probleme als Nägel erscheinen lässt. Ist die Filterinfrastruktur mit ihren Datenbanken und Erkennungs- und Entscheidungsalgorithmen einmal etabliert, drängt sich bei jedem neuen Problem die Frage auf, ob es sich mit Uploadfiltern „lösen" lässt. Und selbstverständlich lassen sich Filtereinstellungen ändern. Einer autoritären Regulierung des Netzes sind damit Tür und Tor geöffnet.

Dass das leider kein dystopischer Alarmismus ist, zeigen andere aktuelle Gesetzgebungsinitiativen. Das EU-Parlament hat gerade ohne Abstimmung die umstrittene Verordnung gegen Terrorpropaganda (TERREG)[12] durchgewunken. Dort konnten zwar unter großem zivilgesellschaftlichem Einsatz in langen Verhandlungen verpflichtende Uploadfilter verhindert werden. Aber insgesamt setzt die Verordnung, unter anderem durch extrem kurze Löschfristen, starke Anreize für ihren „freiwilligen" Einsatz.

Auch der erste Entwurf zum Digital Services Act (DSA-E) will zwar Anbietern keine „allgemeine Verpflichtung" zur automatisierten Überwachung und Überprüfung auf möglicherweise rechtswidrige Inhalte auferlegen. Das schließt spezifische Verpflichtungen und erst recht den „freiwilligen" Einsatz von Filtern aber gerade nicht aus. Vielmehr werden durch strenge Notifizierungsregeln[13] und eine Haftungsfreistellung beim Einsatz freiwilliger Maßnahmen gegen rechtswidrige Inhalte starke Anreize für automatisierte Contentmoderation gesetzt. Angesichts der Reichweite der durch den DSA in den Blick genommenen Regulierung eine beunruhigende Aussicht.

Die Große Koalition hat ihr Versprechen gebrochen

Die Regierungskoalition hat ihre ständig wiederholten Versprechen[14], Uploadfilter nicht einführen zu wollen, mit dem UrhDaG endgültig gebrochen. Dass die Umsetzung dennoch weitgehend geräuschlos erfolgt und die Regierung das UrhDaG mit seinen Uploadfiltern als vernünftigen Ausgleich zwischen den verschiedenen Interessen verkaufen kann, mag in Teilen der Pandemie geschuldet sein. Es liegt aber auch daran, dass sich bereits nach Verabschiedung der Richtlinie viele Menschen vom Thema abgewendet haben – frustriert von wortbrüchigen Politikerinnen und Politikern.

Ausgerechnet die autoritäre PiS-Regierung in Polen hat vor dem Europäischen Gerichtshof Klage gegen die Filterbestimmungen in der EU-Richtlinie erhoben. Eine Entscheidung wird noch im Laufe des Jahres erwartet. Daher könnten die neuen Regelungen schon bald Makulatur werden.

Aber unabhängig vom Ausgang des Verfahrens kann eine selbstbewusste Zivilgesellschaft nicht passiv bleiben. Die Auseinandersetzungen um Uploadfilter und die Regulierung des Internets werden auch in Zukunft nicht nur vor den Gerichten geführt. Das Wahljahr bietet vielfältige Gelegenheiten, die Politik in die Verantwortung zu nehmen. Denn auch wenn die Richtlinie nun umgesetzt wird, haben die Proteste und die Diskussionen der letzten Jahre eindrucksvoll gezeigt, dass Netzpolitik längst kein Nischenthema mehr ist, sondern wahlentscheidend sein kann[15].

Uploadfilter werden nun deutsches Recht. Doch damit sind sie nicht in Stein gemeißelt. Die Bundesregierung hat in ihrer Protokollerklärung[16] zur Verabschiedung der Richtlinie ausdrücklich erklärt, darauf hinzuwirken, dass die Defizite in der EU-Urheberrechtsrichtlinie korrigiert werden müssen, wenn eine Umsetzung weitgehend ohne Uploadfilter nicht möglich sei. Das ist spätestens jetzt der Fall. Selbst wenn der Bundestag nun angesichts der ablaufenden Umsetzungsfrist die vorgeschriebenen Filter einführt: Eine Korrektur auf europäischer Ebene ist jederzeit möglich, wenn der politische Wille da ist.

Der Kampf gegen Uploadfilter geht weiter

Die anstehenden Auseinandersetzungen um die EU-Plattformregulierung bieten dazu die beste Gelegenheit. Denn dort wird die Zukunft der Inhalteregulierung auf Plattformen verhandelt. Der Einsatz von Uploadfiltern muss im DSA kategorisch ausgeschlossen und ein ausgewogenes System entwickelt werden, wie künftig europaweit mit rechtswidrigen Inhalten umzugehen ist. Dazu muss der im Entwurf vorgesehene, richtige Ansatz eines weiterentwickelten Systems von Notice and Action ausgebaut werden.

Auch Urheberrechtsverletzungen sind rechtswidrige Inhalte und könnten unter eine solche Regulierung fallen. Allerdings sieht der Vorschlag der EU-Kommission für den DSA derzeit Ausnahmen für speziellere Regelungen, unter anderem die DSM-RL, aber auch die TERREG vor. Derartige Ausnahmen widersprechen aber der Idee eines einheitlichen Regulierungsrahmens, der die Rechte von Nutzerinnen und Nutzern wahrt. Sie müssen gestrichen werden. Statt eines unübersichtlichen Stückwerks verschiedener Regulierungssysteme, die national zudem teilweise sehr unterschiedliche durchgesetzt werden, sollte der verfehlte Artikel 17 Urheberrechts-Richtlinie und die gescheiterten nationalen Umsetzungen durch eine Lösung innerhalb des DSA als europaweit einheitlicher Regulierungsrahmen ersetzt werden.

Wie schon bei der Urheberrechtsreform wird die Bundesregierung maßgeblichen Einfluss auf die europäische Gesetzgebung haben und hat alle Möglichkeiten, zumindest ihrem Versprechen aus der Protokollerklärung Taten folgen zu lassen. Eine zukünftige Bundesregierung ist also auch daran zu messen, ob sie bereit ist, für die grundlegenden Rechte von Nutzerinnen und Nutzern tatsächlich einzustehen und nicht bloß leere Versprechen zu produzieren. Der Kampf gegen Uploadfilter und gegen eine immer restriktiver konzipierte Regulierung des Internets muss also offensiv weitergeführt werden – auch über das Wahljahr hinaus.

Quelle: https://netzpolitik.org/2021/urheberrechtsreform-uploadfilter-werden-gesetz/

Anmerkungen

1 *Der Beitrag wurde am 20. Mai 2021 veröffentlicht (d. Red.).*
2 *https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019L0790&qid=1619695650734&from=EN*
3 *https://netzpolitik.org/2019/copyfail-eu-parlament-beschliesst-uploadfilter/*
4 *https://www.bundesregierung.de/resource/blob/975226/847984/5b8bc23590d4cb2892b31c987ad672b7/2018-03-14-koalitionsvertrag-data.pdf?download=1*
5 *https://netzpolitik.org/2019/demos-gegen-uploadfilter-alle-zahlen-alle-staedte/*
6 *https://www.sueddeutsche.de/kultur/peter-maffay-urheberrecht-gastbeitrag-1.5252416?reduced=true*
7 *https://www.sueddeutsche.de/kultur/urheberrecht-protest-1.5277804*
8 *https://background.tagesspiegel.de/digitalisierung/an-der-wurzel-des-entsetzens*
9 *https://www.communia-association.org/2021/04/20/open-letter-on-article-17-is-the-commission-about-to-abandon-its-commitment-to-protect-fundamental-rights/*
10 *https://netzpolitik.org/2021/expertenanhoerung-zur-urheberrechtsnovelle-das-beste-das-dem-urheberrecht-passieren-konnte/*

Tom Jennissen

Tom Jennissen arbeitet für die Digitale Gesellschaft[17]. Zu diesem Text haben außerdem Benjamin Bergemann und Volker Grassmuck beigetragen.

11 https://netzpolitik.org/2021/edit-policy-urheberrecht-sportverbaende-lobbyieren-fuer-verschaerfungen/
12 https://netzpolitik.org/2021/terrorpropaganda-eu-gesetz-gegen-terrorinhalte-im-netz-beschlossen/
13 https://edri.org/our-work/delete-first-think-later-dsa/
14 https://digitalegesellschaft.de/2021/03/offener-brief-vertrauen-wiederherstellen-uploadfilter-verhindern
15 https://netzpolitik.org/2019/europawahl-dieser-wahlkampf-wurde-im-internet-entschieden/
16 https://netzpolitik.org/2019/europawahl-dieser-wahlkampf-wurde-im-internet-entschieden/
17 https://digitalegesellschaft.de/

Justus Dreyling

Was hinter dem TRIPS-Waiver steckt

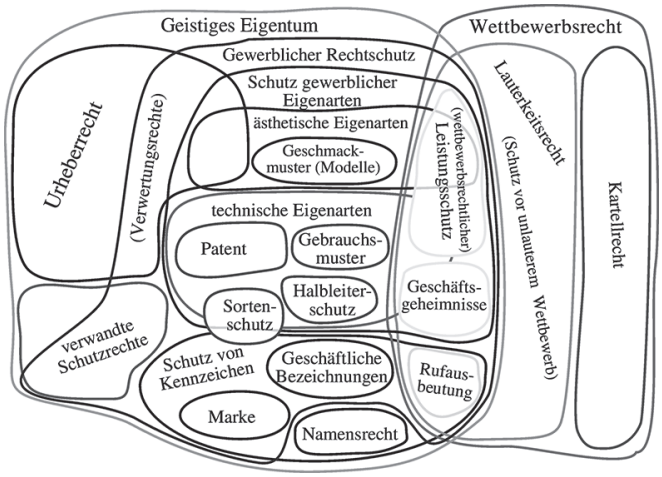
Die USA machen den Weg frei, um den Schutz geistiger Eigentumsrechte für Covid-19-Impfstoffe auszusetzen. Über Zugang zu Medikamenten wird bei der WTO bereits seit über 20 Jahren gerungen. Zu den Hintergründen.

In Deutschland und anderen EU-Mitgliedstaaten scheint dank Impfkampagnen die Rückkehr zu einer – wie auch immer gearteten – Normalität sehr nah. In vielen Entwicklungsländern wie etwa Brasilien und Indien dürfte sich die Lage aufgrund fehlender Impfkapazitäten leider nicht so schnell entspannen.

Frühestens 2023[1] wird nach aktuellen Erwartungen ein akzeptables Impfniveau in den Staaten des globalen Südens erreicht. Ärzte ohne Grenzen befürchtet, dass in diesen Ländern so Virusstämme entstehen könnten, die gegen die aktuellen Impfstoffe immun[2] sind. Auch deshalb fordert eine Koalition von Staaten um Indien und Südafrika seit Oktober 2020 einen temporären Verzicht auf internationale Verpflichtungen für bestimmte geistige Eigentumsrechte.

Der TRIPS-Waiver

Der Antrag[3] mit dem Titel „Verzicht auf einige Bestimmungen des TRIPS-Abkommens zur Prävention, Eindämmung und Behandlung von Covid-19" sieht die Möglichkeit vor, für die Dauer der Corona-Pandemie auf bestimmte geistige Eigentumsrechte zu verzichten. Das betrifft Produkte und Technologien, die zur Prävention, Eindämmung oder Behandlung von COVID-19 beitragen. Insbesondere Entwicklungsländer sollen dadurch in die Lage versetzt werden, etwa Vakzine, Diagnostika oder Therapien rechtzeitig selbst zu produzieren.



Übersicht über verschiedene Arten von Geistigem Eigentum und Verhältnis zum Wettbewerbsrecht – Quelle Cfaerber, CC BY-SA 3.0

Die Industriestaaten, insbesondere die USA und die EU-Mitgliedstaaten, hatten der Forderung nach einem TRIPS-Waiver zunächst eine Absage erteilt. Am Mittwochabend kam es zu einer Kehrtwende.

In einem Statement der US-Handelsbeauftragten Katherine Tai[4] heißt es, „die besonderen Umstände der COVID-19-Pandemie erfordern besondere Maßnahmen". Zwar glaube die US-Regierung um Präsident Joe Biden an geistige Eigentumsrechte, jedoch sei man zur Bekämpfung der Pandemie bereit, Patente und andere relevante geistige Eigentumsrechte auszusetzen, um die weltweite Verfügbarkeit von Impfstoffen zu gewährleisten.

Was ist TRIPS?

Die Abkürzung TRIPS steht für das 1995 in Kraft getretene Abkommen über handelsbezogene Aspekte geistigen Eigentums: Agreement on Trade-Related Aspects of Intellectual Property Rights. Auf Druck der USA, der EU und Japans (und der dort beheimateten Konzerne) wurde TRIPS als einer von drei Pfeilern der neu gegründeten Welthandelsorganisation beschlossen – neben den Freihandelsregeln für Waren (GATT) und Dienstleistungen (GATS).

Das Inkrafttreten von TRIPS bedeutete, dass praktisch alle Staaten bestimmte Standards für den Schutz geistigen Eigentums einhalten mussten. Das TRIPS-Abkommen bündelte dazu viele bestehende Regeln im Bereich des internationalen Immaterialgüterrechts in einem Vertrag. Die Einhaltung der in TRIPS enthaltenen Regeln war nun Bedingung dafür, am internationalen Freihandel teilzunehmen – eine Einnahmequelle, auf die nur wenige Staaten verzichten wollen oder können.

Der Streit um Zugang zu Medikamenten

TRIPS wird seit Vertragsabschluss kontrovers diskutiert[5]. Zuvor konnten Staaten wie Indien Generika[6] produzieren und damit auch andere Staaten des globalen Südens mit wirkstoffmäßig identischen Alternativen zu einem zugelassenen Arzneimittel beliefern. Diese Möglichkeit schränkte TRIPS dramatisch ein.

Bereits 1998 kam es daher zum Knall. Um besser mit den Folgen der HIV-Pandemie umgehen zu können, hatte Südafrika

durch eine Gesetzesänderungen die Ausgabe von Zwangslizenzen für antiretrovirale Medikamente erleichtert. TRIPS sieht Zwangslizenzen gegen angemessene Vergütung („adequate remuneration") explizit als Instrument vor, um die Bereitstellung öffentlicher Güter sicherzustellen – insbesondere, wenn sie der öffentlichen Gesundheit dienen. Staaten können also Hersteller mit der Produktion von Generika beauftragen, sofern sie den eigentlichen Patentinhaber dafür entschädigen. Von dieser Möglichkeit hatten auch Industriestaaten wie Kanada immer wieder Gebrauch gemacht.

Allerdings lief die Pharmaindustrie Sturm gegen die südafrikanische Regierung und legte Verfassungsbeschwerde ein. Auch drohten die USA und die EU Handelssanktionen an, um Südafrika von seinem Kurs abzubringen. Erst unter erheblichem zivilgesellschaftlichem Druck lenkten die Industriestaaten ein. 2001 beschlossen die Mitglieder der WTO die Doha-Erklärung, die die in TRIPS bestehenden Flexibilitäten unterstreicht. Aufgrund der weiterhin bestehenden Sanktionskulisse nahmen jedoch nur wenige Staaten diese Möglichkeit in Anspruch.

Wie geht es nun weiter?

Die Erklärung der US-Regierung, den Weg für den TRIPS-Waiver freizumachen, kam daher überraschend. Ausschlaggebend dürfte auch WTO-Generaldirektorin Ngozi Okonjo-Iweala gewesen sein. Sie hatte immer wieder unterstrichen, wie dringlich die Frage des Zugangs zu Impfstoffen ist[7].

Wie der Waiver allerdings aussehen könnte, ist noch unklar. Die Stellungnahme der US-Handelsbeauftragen bezieht sich auf geistiges Eigentum (und nicht nur Patente) im Zusammenhang mit Impfstoffen, was Spielraum für Interpretation lässt. Sie ist aber enger gefasst als der ursprüngliche Vorschlag von Indien und Südafrika, der neben Impfstoffen auch Medikamente und Technologien zur Behandlung von Infektionen sowie Tests einschloss.

„Der nächste Schritt sind textbasierte Verhandlungen, um den tatsächlichen Waiver auszugestalten, sobald alle WTO-Mitglieder sich dazu bereit erklären", erklärt Sean Flynn, Direktor des Program on Information Justice and Intellectual Property an der American University in Washington, D.C. „Zum gegenwärtigen Zeitpunkt blockieren allerdings einige wichtige WTO-Mitglieder den Übergang zu textbasierten Verhandlungen. Diese Mitglieder werden von ihrer Position abweichen müssen. Das Thema könnte ansonsten auch durch eine Abstimmung forciert werden, was in der WTO allerdings nur sehr selten geschieht."

Einige EU-Mitgliedstaaten schlossen sich der US-Position am Donnerstagmorgen an, darunter Frankreich. Die Bundesregierung äußerte sich bislang eher zurückhaltend. Kommissionspräsidentin Ursula von der Leyen gab auf Twitter bekannt[8], den Vorschlag der USA erörtern und zu einer pragmatischen Lösung gelangen zu wollen. Wie eine gemeinsame Position der EU-Mitgliedstaaten aussehen könnte, ist zur Stunde aber noch offen.

Zivilgesellschaftliches Engagement

Bei den Verhandlungen steckt der Teufel im Detail. Die Pharmaindustrie torpediert den Vorschlag seit Monaten und wird sich für möglichst weiche Bestimmungen einsetzen. Auch Vertreter:innen der Filmindustrie in den USA sprachen sich gegen den Waiver aus[9], da sie eine Ausweitung auf das Urheberrecht befürchten.

Deshalb wird es nun auf das zivilgesellschaftliche Engagement von Organisationen ankommen, die sich bereits seit vielen Jahren für Zugang zu Medikamenten aussprechen wie etwa Ärzte ohne Grenzen[10] oder Knowledge Ecology International[11]. Das Wissen über Impfstoffe und Therapien ist der Schlüssel, um die Pandemie zu beenden. Aus diesem Grund unterstützt auch Wikimedia Deutschland[12] die Forderungen nach einem TRIPS-Waiver.

Quelle: https://netzpolitik.org/2021/streit-um-impfstoff-patente-was-hinter-dem-trips-waiver-steckt/

Anmerkungen

1 *https://www.eiu.com/n/eiu-latest-vaccine-rollout-forecasts/*
2 *https://www.aerzte-ohne-grenzen.de/faq/1927*
3 *https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/IP/C/W669.pdf*
4 *https://ustr.gov/about-us/policy-offices/press-office/press-releases/2021/may/statement-ambassador-katherine-tai-covid-19-trips-waiver*
5 *https://netzpolitik.org/2021/kommentar-patente-helfen-nicht-gegen-pandemien/*
6 *https://de.wikipedia.org/wiki/Generikum*
7 *https://www.wto.org/english/news_e/news21_e/gc_05may21_e.htm*
8 *https://twitter.com/vonderleyen/status/1390214897322139648*
9 *https://theintercept.com/2021/04/27/covid-vaccine-copyright-hollywood-lobbyists/*
10 *https://www.aerzte-ohne-grenzen.de/presse/europa-covid-19-impfstoff-patentausetzung*
11 *https://www.keionline.org/36102*
12 *https://www.wikimedia.de/presse/pandemiebekaempfung-wikimedia-deutschland-fordert-aussetzbarkeiten-restriktiver-handelsregeln-in-krisenlagen/*
13 *https://netzpolitik.org/tag/blackbox-genf/*

Justus Dreyling

Justus Dreyling ist promovierter Politikwissenschaftler und seit 2019 bei *Wikimedia* für internationale Regelsetzung zuständig. Vorher hat er am Otto-Suhr-Institut der Freien Universität Berlin zum Handel und zu internationalen Regeln für geistiges Eigentum geforscht. Er twittert als *@3_justus* und berichtet in der Reihe *Blackbox Genf13* von den Verhandlungen bei der *Weltorganisation für geistiges Eigentum* (WIPO).

Markus Reuter

Trotz Digitalisierungsschub noch gravierende Lücken

Die Lehrer:innengewerkschaft GEW hat Anfang des Jahres eine repräsentative Umfrage zur Digitalisierung an deutschen Schulen durchgeführt. Das Ergebnis: Deutschland kommt langsam auf dem internationalen Stand von 2018 an.

Die Pandemie hat zu einem enormen Digitalisierungsschub an deutschen Schulen geführt und die Defizite aus vorpandemischen Zeiten abgemildert. Dennoch klafften weiterhin „eklatante" Digitalisierungslücken, hat eine Studie der Lehrer:innengewerkschaft GEW[1] ergeben. So gibt es zum Beispiel an 30 Prozent der Schulen kein WLAN für die Lehrer:innen und an 50 Prozent keines für die Schüler:innen.

Die Digitalisierungslücke zieht sich laut der repräsentativen Studie durch alle Bereiche. Nur an gut der Hälfte aller Schulen gibt es ausreichend digitale Geräte im Unterricht. Ähnlich sieht die Situation für die Lehrer:innen aus: Weil diese nicht genügend Endgeräte zur Verfügung gestellt bekommen, nutzen 95 Prozent öfter ihre eigenen Smartphones, Tablets und Computer für die Arbeit als vor der Pandemie.

Mit milliardenschweren Paketen wie dem DigitalPakt Schule[2] und Folgeprogrammen[3] versucht die Bundesregierung seit einigen Jahren, die deutschen Defizite in der Digitalisierung zu beseitigen. Tatsächlich lässt sich trotz der Anlaufschwierigkeiten ein Aufholen beobachten: 2018 hatten fast 85 Prozent aller Lehrer:innen keinen tragbaren Arbeitsrechner, obwohl international schon jede zweite Lehrkraft mit einem solchen ausgerüstet war. Bis 2020 waren schließlich knapp 40 Prozent der Lehrenden digital ausgestattet, ein Jahr später fast die Hälfte. Ein großes Problem sei jedoch, dass in nur der Hälfte der Schule die Lehrer:innen auf technische Unterstützung bauen können. Das führe zu erhöhten Arbeitsaufwänden durch die Digitalisierung, heißt es in der Studie.

Jetzt erst auf internationalem Stand von 2018

Immerhin gehört der Einsatz digitaler Medien mittlerweile in 90 Prozent der Fälle zum Unterrichtsgeschehen. Digitale Schulbücher werden aber nur in der Hälfte der Fälle eingesetzt. Auffällig ist, dass Deutschland im internationalen Vergleich in vielen Feldern erst jetzt auf dem Stand ist, der international schon 2018 erreicht wurde. Aktuelle Zahlen über den heutigen Stand der anderen Länder liegen noch nicht vor.

„Die Lehrkräfte müssen sich auf die pädagogischen Aufgaben konzentrieren können", mahnt deswegen Ilka Hoffmann, GEW-Vorstandsmitglied Schule, an[4]. „Wir brauchen endlich mehr IT-Fachleute für den technischen Support, die Gelder für die Ein-

stellung etwa von Systemadministratoren stehen bereit. Diese Mittel müssen endlich abgerufen und verstetigt werden. Digitale Werkzeuge sollen die Lehrkräfte pädagogisch unterstützen – und nicht zu einer Dauerbaustelle werden."

Neueste Zahlen zeigen, dass die digitalen Corona-Hilfen für die Schulen nur schleppend anlaufen und Gelder bis heute noch nicht abgerufen[5] werden. Der Anteil der Lehrkräfte mit sehr geringer und geringer Digitalkompetenz liegt je nach Schule zwischen 43 und 53 Prozent. Hier werden große Unterschiede zwischen Schulen sichtbar, die bei der Digitalisierung Vorreiter sind und jenen, welche die Studie als „Nachzügler" bezeichnet. An diesen Schulen ist die digitale Ausbildung der Schüler:innen deutlich schlechter.

Quelle: https://netzpolitik.org/2021/schul-studie-trotz-digitalisierungsschub-noch-gravierende-luecken/

Anmerkungen

1 *https://www.gew.de/fileadmin/media/sonstige_downloads/hv/Service/Presse/2021/Digitalisierung-im-Schulsystem---Studie.pdf*
2 *https://netzpolitik.org/tag/digitalpakt-schule/*
3 *https://netzpolitik.org/2021/sondervermoegen-digitale-infrastruktur-troepfelnder-geldhahn-fuer-deutschlands-schulen/*
4 *https://www.gew.de/presse/pressemitteilungen/detailseite/neuigkeiten/gew-trotz-digitalisierungsschub-eklatante-technikluecken-ungleichheiten-und-starke-belastung-der-leh/*
5 *https://netzpolitik.org/2021/digitalpakt-schule-corona-hilfen-fuer-schulen-kommen-nur-schleppend-an/*

Markus Reuter

Markus Reuter beschäftigt sich mit den Themen Digital Rights, Hate Speech & Zensur, Fake News & Social Bots, Rechtsradikale im Netz, Videoüberwachung, Grund- und Bürgerrechte sowie soziale Bewegungen. Bei *netzpolitik.org* seit März 2016 als Redakteur dabei. Er ist erreichbar unter *markus.reuter | ett | netzpolitik.org* und auf Twitter unter *@markusreuter_*

Pia Stenner

Corona-Hilfen für Schulen kommen nur schleppend an

Mit drei Zusatzprogrammen wollte der Bund Schulen in der Pandemie bei der Digitalisierung helfen. Doch eine Nachfrage bei den Bundesländern ergibt: Die meisten Lehrkräfte haben aber noch immer keine Dienstlaptops und für die Verbesserung der IT-Administration sind offenbar noch keine Mittel abgerufen worden.

Der Digitalpakt Schule ist ein fünf Milliarden schweres Projekt des Bundesministeriums für Bildung und Forschung (BMBF), das von 2019 bis 2024 deutsche Schulen digitaler machen soll. Dann wurden in der Pandemie die digitalen Defizite der Schulen noch deutlicher. Deswegen sollten Zusatzpakete von je 500 Millionen Euro die Lücken stopfen. Doch während die Schulen jetzt allmählich wieder in den Präsenzbetrieb übergehen, werden Teile dieser Zusatzpakete noch immer nicht abgerufen.

Fünf Milliarden und drei Corona-Hilfen

Die Verwaltungsvereinbarung „Digitalpakt Schule“[1] wurde 2019 beschlossen und fußt auf der Änderung im Grundgesetz[2], die dem Bund Finanzierungshilfen den ansonsten den Ländern vorbehaltenen Bildungsbereich erlaubt. Die Länder steuern einen Eigenanteil von mindestens zehn Prozent bei. Förderwürdig durch den Digitalpakt sind beispielsweise Schulserver, schulisches WLAN, Lernplattformen oder interaktive Tafeln.

Die Zusatzverwaltungsvereinbarung „Sofortausstattungsprogramm“[3] oder „Corona-Hilfe I“ wurde im Juli 2020 beschlossen, um Schüler:innen, die zuhause keinen Computer haben, ein mobiles Endgerät für den Distanzunterricht zur Verfügung zu stellen und Schulen bei Online-Lehrinhalten zu unterstützen.

Darauf folgte im Dezember 2020 die „Corona-Hilfe II“, die Zusatzverwaltungsvereinbarung „Administration“[4]. Die 500 Millionen Euro aus diesem Paket sollen in die Ausbildung und Finanzierung von IT-Administrator:innen an Schulen fließen. Förderfähig sind hier „befristete Ausgaben für Personalkosten […] für professionelle Administrations- und Support-Strukturen“ sowie „pauschalierte Zuschüsse zu Ausgaben für die Qualifizierung und Weiterbildung“ von IT-Administrator:innen, die bei den Ländern oder Schulträgern angestellt sind.

Als „Corona-Hilfe III“ beschloss der Bund mit den Ländern Anfang 2021 dann eine dritte Zusatzverwaltungsvereinbarung: „Leihgeräte für Lehrkräfte“[5]. „Angesichts der pandemiebedingten Ausnahmesituation“ heißt es in der Vereinbarung, wolle man mit 500 Millionen Euro aus diesem Programm Laptops, Notebooks oder Tablets für Lehrkräfte zur Verfügung stellen.

Die Länder müssen dem Bund regelmäßig berichten, wie viele Mittel aus dem Digitalpakt und seinen Zusatzprogrammen abgeflossen sind. Der letzte Stichtag war im Dezember 2020. Aus dem Sofortausstattungsprogramm hatten acht Bundesländer ihre Anteile vollständig abgerufen, in weiteren Bundesländern zumindest große Teile. Nur in Thüringen lag der absolute Mittelabfluss zum 31. Dezember[6] noch bei Null Euro. Das „Leihgeräte für Lehrkräfte“-Programm war zu diesem Zeitpunkt noch nicht beschlossen, doch auch aus dem Administrations-Programm gab es noch keinen Mittelabfluss.

Bundesländer wenig auskunftsfreudig

Deshalb haben wir die 16 Kultusministerien der Länder nach dem aktuellen Stand bei der Umsetzung der sogenannten Zusatzverwaltungsvereinbarungen zum Digitalpakt Schule gefragt. Nach drei Wochen hat knapp die Hälfte der Länder immer noch nicht geantwortet. Doch auch unter den Ländern, die geantwortet haben, zeigen sich teils große Unterschiede.

Die Umsetzung des Sofortausstattungsprogramms scheint in den meisten Ländern weiter gut voranzugehen oder bald abgeschlossen zu sein: Hessen hat 85.000 Geräte bis Ende April ausgeliefert, in Rheinland-Pfalz[7] konnten 57.000 Geräte angeschafft werden, in Sachsen wurden rund 47.000 Geräte beschafft. Doch die Zahlen aus den verschiedenen Ländern sind schwer vergleichbar – nicht nur, weil jedem Land eine andere Summe zusteht.

Aus Bayern heißt es, „bis Ende 2020 war bereits ein großer Teil der Schülerleihgeräte tatsächlich bei den Schülerinnen und Schülern angekommen.“ Baden-Württemberg berichtet, dass 130 Millionen Euro direkt an die Schulträger überwiesen worden seien. Auch Nordrhein-Westfalen nennt keine Zahl der Geräte, weil die Schulträger zuständig seien, jedoch eine Gesamtsumme von 255 Millionen Euro[8], die für Lehrer- und Schülergeräte zusammen beantragt worden seien. Sachsen-Anhalt schätzt, dass es rund 22.000 Geräte sind. „Genauere Zahlen liegen noch nicht vor“, heißt es mit der Begründung, dass man einen zentralen IT-Landesdienstleister mit der Gerätebeschaffung beauftragt habe, sich aber dennoch einzelne Schulträger selbst um die Anschaffung kümmern.

Gewerkschaft: „Reibungsverluste“

Jedes Land gestaltet die Umsetzung der Bundeshilfen ein bisschen anders – genau wie die Verteilung der Zuständigkeiten zwischen Land und Schulträger. Die Lehrerin Ilka Hoffmann leitet in der Gewerkschaft Erziehung und Wissenschaft (GEW)[9] den Organisationsbereich Schule. Sie meint: „Die Zuständigkeiten sind über zu viele Ebenen verteilt, dabei entstehen Reibungsverluste.“ Ihr sei ein Fall bekannt, da habe eine Schule über die 60 bedürftige Schüler:innnen gemeldet, damit sie über das Sofortausstattungsprogramm Geräte für den Distanzunterricht bekommen. „Dann muss das aber geprüft werden, und am Ende bekam die Schule nur ein Gerät“, erzählt Hoffmann.

Aus ihrer Sicht dauert die Umsetzung der Corona-Hilfen zu lange. „Die Verwaltungsvorschriften des Bundes müssen vom Land erst in Durchführungsverordnungen umgesetzt werden und die Schulen müssen medienpädagogische Konzepte bei den Schulträgern vorlegen.“ Aus Hoffmanns Sicht sind das überbürokratisierte Abläufe. „Man muss über diese Art des Förderalismus nachdenken“, sagt sie.

Das jüngste Zusatzpaket des Bundes, „Leihgeräte für Lehrkräfte", steht in den meisten Ländern, die sich auf unsere Anfrage zurückmeldeten, noch ganz am Anfang. In Brandenburg ist „die Antragstellung demnächst möglich", in Rheinland-Pfalz kann das Antragsverfahren „alsbald starten." In anderen Ländern wie Bayern oder Baden-Württemberg sind Anträge schon bewilligt und Geräte bestellt, doch man rechnet nicht damit, dass sie vor Beginn des kommenden Schuljahres ankommen.

In Hessen wurden die ersten Lehrergeräte schon am 30. März übergeben, darüber berichtet das hessische Kultusministerium in einer Pressemitteilung[10]. Aus einer kleinen Anfrage der SPD[11] in Hessen geht aber hervor, dass es sich wohl nur um eine symbolische Übergabe von zwei Geräten gehandelt habe. „Bis die Geräte schlussendlich genutzt werden können, wird es aufgrund der notwendigen Einrichtung noch vier Monate dauern", schreiben die SPD-Landtagsabgeordneten Kerstin Geis und Bijan Kaffenberger.

Kaffenberger ärgert sich, dass von der Landesregierung wenig unternommen werde, um die Umsetzung der Coronahilfen aus dem Digitalpakt zu beschleunigen. „Lehrkräfte sind Angestellte des Kultusministeriums. Wenn ich im hessischen Kultusministerium arbeite, und da steht kein Laptop, kann ich zurecht sagen: Ich kann nicht arbeiten." Es sei inakzeptabel, dass Lehrer:innen Privatgeräte für Unterrichtsvorbereitung, Korrekturen von Klassenarbeiten, Beurteilungen, Korrespondenz mit Eltern und vielleicht sogar schulpsychologische Gutachten nutzen. „Deswegen ist es gut, dass die Geräte jetzt kommen und der Bund das mal angestoßen hat", meint Kaffenberger.

Für den Distanzunterricht zu spät

Den privaten Computer, mit dem der Lehrer Stefan Düll von zuhause aus arbeitet, wird ein neues Gerät aus der Zusatzprogramm des Digitalpakts aber gar nicht ersetzen. Stefan Düll ist der stellvertretende Vorsitzende des deutschen Philologenverbandes (DPHV)[12] und leitet ein Gymnasium im Landkreis Augsburg. „Allein schon ergonomisch sind die kleinen Laptops gar nicht dafür gedacht, länger daran zu arbeiten und zum Beispiel den Unterricht vorzubereiten", meint Düll.

„Als digitale Stütze für den Präsenzunterricht" seien die Geräte sinnvoll. „Für den Distanzunterricht kommen sie ja sowieso zu spät", sagt Düll. Kameras oder Mikrofone als Ergänzung für ältere Rechner mit Desktop hätten sich die meisten Lehrer:innen im vergangenen Jahr ohnehin längst selbst gekauft, um den Unterricht als Videokonferenz abhalten zu können. Warum konnten Bund und Länder im vergangenen Jahr hier nicht schneller aushelfen? Liegen zu viele bürokratische Hürden zwischen Bedarf der Lehrkräfte und Hilfe der Politik? „Man kann nicht einfach irgendwie blind die Steuergelder raushauen", meint Stefan Düll. Die einzelnen Beantragungs- und Bewilligungsprozesse dienten schließlich dem Zweck, dass die Mittel auch wirklich ankommen.

Doch genau diese Prozesse laufen nicht in jedem Bundesland gleich ab. Mal liegt mehr Verantwortung beim Land, mal mehr Verantwortung bei den Schulträgern. Und wer ist überhaupt Schulträger? Mal sind es Landkreise, mal große Kommunen, mal Zusammenschlüsse von Gemeinden, in Hamburg ist das Land selbst Schulträger. Je nachdem verfügen die Schulträger über ganz unterschiedliche Voraussetzungen, sich um die Digitalisierung an ihren Schulen zu kümmern, meint Ilka Hoffmann von der GEW.

Zentrale Beschaffung wäre besser gewesen

„Manche Kommunen mit dem Personal und der Erfahrung im Rücken kriegen das super hin, aber gerade in kleinen, ärmeren Kommunen klemmt es oft", sagt sie. Und in manchen Kommunen fehle einfach die Bereitschaft, sich um die Schulen intensiv zu kümmern. „Danach sehen manche Schulen ja auch aus. Eine ziemliche Schande." Das gleiche Problem spricht Bijan Kaffenberger an. Aus seiner Sicht hätte die hessische Landesregierung die Beschaffung der Geräte zentral organisieren und nicht den Medienzentren auf Kreis- oder kommunaler Ebene überlassen sollen.

„Das Land hätte die Medienzentren außerdem schon längst personell massiv stärken müssen", meint Kaffenberger. Die hessischen Medienzentren werden von den Schulträgern betrieben, doch das Land zahlt die Lehrkräfte, die dort arbeiten. Kaffenberger sagt, diese seien schon mit der Einrichtung der Sofortausstattungsgeräte für die Schüler:innen überfordert gewesen. „Es wurde ein Schritt vor den anderen gemacht, indem man die Geräte anschafft, bevor die Administrationsleistung da ist."

Und die Administration? „Keine abschließenden Informationen"

Bei den Mitteln aus der Corona-Hilfe für die Administration sieht es in Sachen Abruf der Gelder bislang düster aus: „Zu dieser Fördermaßnahme gibt es noch keine Anträge oder Bezuschussungen", heißt es aus Sachsen-Anhalt. „Es laufen derzeit noch letzte Abstimmungen zum Supportprogramm. Voraussichtlich im Juni kann die Förderrichtlinie in Kraft treten", teilt hingegen das hessische Kultusministerium mit.

Bayern schreibt: „Die bayerische Richtlinie ist fertiggestellt und befindet sich in der finalen Abstimmung mit dem Bundesministerium für Bildung und Forschung." Baden-Württemberg teilt mit: „Hierzu liegen dem Kultusministerium aktuell keine abschließenden Informationen vor." Nur das Schulministerium NRW berichtet von 5,6 Millionen Euro, die nordrhein-westfälische Schulträger inzwischen aus dem Förderprogramm beantragt hätten.

Pia Stenner

Pia Stenner ist von Mitte April bis Mitte Juli als Praktikantin bei *netzpolitik.org* und studiert Journalistik und Politikwissenschaft an der TU Dortmund. Sie interessiert sich besonders für Digitales, das mit Politik, Medien und Gesellschaft zusammenhängt.

Geeignetes IT-Personal sei auf dem Markt sehr knapp, sagt Stefan Düll vom DPhV. Das Problem bestätigt auch Ilka Hoffmann von der GEW. Die Bezahlung im öffentlichen Dienst sei nicht so gut wie in der freien Wirtschaft. „Wer nimmt da irgendeine halbe Stelle an einer Kommune?" Dazu sei der Spagat zwischen „technisch möglich" und „didaktisch erwünscht" für IT-Personal ohne pädagogischen Hintergrund nervenaufreibend.

Vielerorts übernehmen derzeit Lehrkräfte gegen ein paar Unterrichtsstunden weniger die vollständige IT-Administration ihrer Schulen und kommen damit an ihre Belastungsgrenze, wie wir am Fall eines Lehrers aus Baden-Württemberg[13] berichteten. Stefan Düll gibt sich optimistisch, dass sich daran durch das Adminstrations-Programm bald etwas ändert. „In Bayern laufen gerade die Gespräche zwischen Landkreisen und IT-Firmen, an die man die Administration outsourcen kann." Es gehe eben nicht immer alles so schnell wie gewünscht, man sei jedoch auf einem „verdammt guten Weg".

Corona-Hilfen für mehr Digitalisierung nach Corona

Ein Weg, der sich in die Länge zieht – vermutlich über das Ende der Pandemie hinaus. Die Laptops für Lehrer:innen werden zum Großteil erst zum Einsatz kommen, wenn der Unterricht längst wieder in Präsenz stattfindet. Mit „Corona-Hilfen", wie das BMBF die Zusatzprogramme des Digitalpakts auf seiner Webseite nennt, haben die Fördermittel dann nicht mehr viel zu tun.

Der hessische Digitalpolitiker Bijan Kaffenberger sagt jedoch: „Es ist unglaublich wichtig, dass wir das Thema Digitalisierung an Schulen jetzt nicht als ein rein pandemisches begreifen." So müsse dringend auch die Frage geklärt werden, wer Support und Wartung von jetzt beschafften Geräte langfristig finanziere. Die Pandemie habe Probleme aufgezeigt, die es bei der Digitalisierung an deutschen Schulen schon lange gibt, meint Stefan Düll. „Lehrer mussten sich bisher immer privat darum kümmern, wenn es darum geht, digitaler zu werden." Das ändert sich jetzt. Aber sehr langsam.

Quelle: https://netzpolitik.org/2021/digitalpakt-schule-corona-hilfen-fuer-schulen-kommen-nur-schleppend-an/

Anmerkungen

1 *https://www.digitalpaktschule.de/files/VV_DigitalPaktSchule_Web.pdf*
2 *https://www.gesetze-im-internet.de/gg/art_104c.html*
3 *https://www.digitalpaktschule.de/files/Zusatzvereinbarung-web.pdf*
4 *https://www.digitalpaktschule.de/files/2020-11-03_ZV_Administration_web.pdf*
5 *https://www.digitalpaktschule.de/files/ZV%20Leihgeräte%20für%20Lehrkräfte%20DPS%202019%20bis%202024.pdf*
6 *https://www.digitalpaktschule.de/de/die-finanzen-im-digitalpakt-schule-1763.html*
7 *https://bm.rlp.de/de/service/pressemitteilungen/detail/news/News/detail/digitalmittel-des-bundes-kommen-im-land-an/*
8 *https://www.schulministerium.nrw/presse/pressemitteilungen/ministerin-gebauer-wir-unterstuetzen-die-schultraeger-beim-abruf-der*
9 *https://www.gew.de/hauptvorstand/ob-schule/*
10 *https://digitale-schule.hessen.de/pressemitteilungen/erste-tablets-und-laptops-für-lehrkräfte-ausgeliefert*
11 *http://starweb.hessen.de/cache/DRS/20/1/05491.pdf*
12 *https://www.dphv.de/dphv/vorstand/*
13 *https://netzpolitik.org/2021/schul-it-in-baden-wuerttemberg-das-grosse-chaos/*

Constanze Kurz

Merkels Geheimdienst-Bla-Bla-Blamage

Es gibt neue brisante Enthüllungen über geheimdienstliche Überwachung, die es eigentlich nicht geben dürfte. Aber nach ein bisschen öffentlicher Verharmlosung und Beschwichtigung gehen wieder alle zur Tagesordnung über. Doch es geht gar nicht um abgehörte Spitzenpolitiker, sondern um aufgeblähte Geheimdienstapparate, die niemand kontrolliert. Ein Kommentar.

Aus den Papieren von Edward Snowden wissen wir, dass die Five Eyes in Europa mit neun Staaten enger zusammenarbeiten als mit anderen. Wer geographisch günstig liegt, politisch halbwegs opportun ist und technisch nicht in der Kreisliga spielt, bei dem klopfte der US-amerikanische Geheimdienst NSA irgendwann an, um eine Zusammenarbeit einzuleiten. Denn vierzehn Augen sehen bekanntlich mehr als fünf Augen.

Zu diesem Verbund, der SIGINT Seniors Europe (SSEUR) genannt wird, gehören neben Deutschland auch Belgien, Frankreich, Italien, die Niederlande, Norwegen, Schweden und Spanien. Außerdem dabei ist Dänemark, das aktuell im Zentrum eines Geheimdienstskandals steht, den Journalisten enthüllt haben[1]. Dabei wurde das Vorgehen beschrieben, wie das Abhören und Auswerten des Internetverkehrs an dänischen Netz-Knotenpunkten ablief – nach dortigen Gesetzen übrigens rechtswidrig.

Der technische Geheimdienst NSA, der 1952 gegründet wurde, sollte eigentlich mal den damaligen Erzfeind der US-Amerikaner belauschen, die Sowjetunion. Fast siebzig Jahre später ist die Sowjetunion längst Geschichte, und die Überwachungsziele sind nicht mehr die Feinde der Vereinigten Staaten, sondern Partner und Alliierte, sogar Freunde. Aktuell half der dänische Militärgeheimdienst Forsvarets Efterretningstjeneste (FE)[2] der NSA beim Belauschen auch von deutschen Politikern.

Die dänischen Geheimen nutzen auch das NSA-Spionageprogramm XKeyscore[3], welches eine Durchsuchung von Daten aus verschiedenen riesigen Datenbeständen erlaubt. Das war schon länger bekannt. Denn Dänemark gehört zu den zwei europäischen Staaten, in denen die vormals geheimen Praktiken im geheimdienstlichen Niemandsland und konkret auch die NSA-Selektoren wenigstens mal geprüft wurden.

Dass auch der neuerliche Skandal nur die Spitze des Eisbergs ist, braucht man nicht mal mehr zu betonen, weil es ohnehin jeder weiß. Es gibt keinen Grund anzunehmen, dass es so oder ähnlich nicht auch bei allen anderen Geheimdienst-Kooperationen läuft. Es gab nur noch keinen Whistleblower, der sein Wissen an die Presse gegeben hätte. Zudem ist seit Beginn der Snowden-Veröffentlichungen die Geheimdienst-Überwachung nicht etwa weniger geworden, sondern signifikant mehr.

Auch der BND spähte unter Freunden

Wir lernen: Mal wieder fliegt ein Skandal in der Kategorie „Ausspähen unter Freunden" auf, den es eigentlich nicht geben dürfte.

Krokodilstränen würde der belauschten Bundesregierung aber wohl keiner abnehmen: Denn der BND überwachte mit eigenen Selektoren das Innenministerium von Dänemark, wie der Spiegel im Jahr 2015 offenlegte[4]. Das geschah teilweise im Auftrag der NSA, aber nicht nur: Der BND nutzte eben auch seine eigenen Überwachungsselektoren, wie später rauskam. Auch die Botschaften fast aller EU-Staaten in Berlin mitsamt der Konsulate im Bundesgebiet – einschließlich der von Dänemark – belauschte der BND jahrelang und systematisch[5].

Vielfach wurde jetzt wieder Angela Merkels Ausspruch zitiert, den sie vor dem EU-Gipfel im Oktober 2013 machte:

> *„Ausspähen unter Freunden – das geht gar nicht".*

Dass ihr eigenes Mobiltelefon abgehört worden war, prägte damals die internationalen Schlagzeilen und ließ die mächtige Regierungschefin wie eine technische Amateurin ohne politisches Gewicht dastehen. Sie betonte, das hätte sie dem damaligen US-Präsidenten Barack Obama zuvor telefonisch ausgerichtet und auf eine vertrauensvolle Beziehung gepocht.

Vergessen hingegen scheint aber, was Merkel gleich im nächsten Satz betonte. Dass es ihr nämlich nicht um ihr persönliches Telefon ginge, sondern darum, dass Ausspähen unter Freunden gegenüber niemandem legitim sei:

> *„Das gilt für jeden Bürger und jede Bürgerin in Deutschland. Dafür bin ich als Bundeskanzlerin auch verantwortlich, das durchzusetzen".*

Diesem Versprechen folgten bis heute keine Taten. Man mag das noch irgendwie einsehen unter einem Mann wie Donald Trump. Für den neuen Präsidenten Biden gilt diese Ausrede aber nicht mehr, schon gar nicht, wenn er sich offenbar im Gegensatz zu seinem Vorgänger wieder freundschaftlich an Deutschland und Europa anzuschmiegen plant.

Wie wäre es denn, wenn die Bundeskanzlerin genau das von Biden nun öffentlich fordern würde, damit sich jeder Bürger und jede Bürgerin in Deutschland wieder sicher sein könnte, nicht von Freunden ausgespäht zu werden? Wahlweise wäre ich auch damit zufrieden, wenn Annalena Baerbock oder zur Not auch Armin Laschet das fordern würden.

Kontrolle der Geheimdienste durch Whistleblower und Journalisten

Damit wäre es aber nicht getan, denn Geheimdienste demokratisch zu kontrollieren, ist und bleibt eine Chimäre. Das wissen wir spätestens seit dem BND-NSA-Untersuchungsausschuss, der sich ab 2014 intensiv mit den Geheimdiensten und deren Praktiken beschäftigt hat. Alles ist streng geheim, und dass die Öffentlichkeit überhaupt eine Ahnung hat, was abertausende Analysten technisch treiben, verdanken wir letztlich Whistleblowern und Journalisten.

Wer einmal gedacht hatte, dass die ans Licht gekommenen Geheimdienstpraktiken doch nicht ohne ernsthafte Reaktionen bleiben könnten, wurde nicht nur enttäuscht, sondern musste in Deutschland dabei zusehen, wie der BND personell, finanziell und was seine rechtlichen Rahmenbedingungen angeht sogar noch erheblich aufgerüstet[6] wurde.

Mehr als Verharmlosungen und Beschwichtigungen, die auch nach den aktuellen Enthüllungen wieder verlautbart wurden, sind von den verantwortlichen Spitzenpolitikern nicht zu hören. Im Zentrum der Kommentare stehen die prominenten Abhöropfer, und eben nicht die Millionen namenlosen Menschen, nach deren anlassloser Überwachung[7] kein Hahn mehr kräht. Dabei können wir davon ausgehen, dass in der Nach-Snowden-Zeit neben Deutschland auch so einige andere Staaten erheblich aufgerüstet haben. Schließlich gab es technisch einiges aufzuholen.

Dieser Spirale der technischen, aber auch rechtlichen und personellen Aufrüstung muss endlich Einhalt geboten werden. Das gilt auch in Deutschland für das BND-Gesetz, mit dessen Novelle ein bisher nicht gekanntes Ausmaß an Überwachung legalisiert wurde. Vielleicht könnten wir bei dieser Gelegenheit auch das BND-Budget, das seit Snowden mal eben auf über eine Milliarde verdoppelt wurde, wieder auf ein Maß zurückschrauben, das einer Demokratie würdig ist? Nach der Pandemie gäbe es sicher mehr als genug Ideen, wer die wahnwitzig hohe Summe besser brauchen könnte.

Im Übrigen bin ich der Meinung, dass Deutschland Edward Snowden endlich Asyl gewähren sollte.

Quelle: https://netzpolitik.org/2021/ausspaehen-unter-freunden-merkels-geheimdienst-bla-bla-blamage/

Anmerkungen

1 *https://www.tagesschau.de/investigativ/ndr-wdr/nsa-bespitzelung-politiker-101.html*
2 *https://de.wikipedia.org/wiki/Forsvarets_Efterretningstjeneste*
3 *https://de.wikipedia.org/wiki/XKeyscore*
4 *https://magazin.spiegel.de/EpubDelivery/spiegel/pdf/139688827*
5 *https://netzpolitik.org/2017/spionage-unter-freunden-der-bnd-hat-eine-geschichte-der-unterwanderung/*
6 *https://netzpolitik.org/2020/bnd-gesetz-eine-neue-lizenz-zum-hacken/*
7 *https://netzpolitik.org/2020/was-heisst-quellenschutz-im-zeitalter-digitaler-massenueberwachung/*

Infos zur Autorin siehe Seite 57

Constanze Kurz

Menschenrechtsgerichtshof schränkt Massenüberwachung der Geheimdienste ein

Der Europäische Menschenrechtsgerichtshof in Straßburg hat heute die britische geheimdienstliche Massenüberwachung als Verstoß gegen Menschenrechte gebrandmarkt. Mit dem Urteil der Großen Kammer kommen neue Anforderungen auf die Gesetzgeber aller europäischen Staaten zu, die solche Massenüberwachung betreiben. Auch der Schutz von Journalisten muss sich verbessern. Ein Kommentar.

Europäischer Gerichtshof für Menschenrechte (Straßburg) – Foto: CherryX, CC BY-SA 3.0

Der Europäische Menschenrechtsgerichtshof[1] in Straßburg hat heute[2] sein Urteil zur geheimdienstlichen Massenüberwachung bekanntgegeben. Da ich einer der Beschwerdeführer in diesem Fall war, kann ich nicht objektiv über die Entscheidung schreiben. Einen Kommentar aber muss ich loswerden.

Zunächst das heutige Urteil des Menschenrechtsgerichtshofs[3] in aller Kürze: Artikel 8 der Europäischen Menschenrechtskonvention (Menschenrecht auf Achtung des Privat- und Familienlebens) sowie Artikel 10 (Menschenrecht auf Freiheit der Meinungsäußerung) wurden beide durch die Massenüberwachung der britischen Geheimdienste verletzt. Die Richter legten wegen des Verstoßes gegen die Menschenrechte und um dem Missbrauch der Datenhalden entgegenzuwirken neue Anforderungen fest, die künftig für alle Staaten gelten, die der Konvention beigetreten sind.

Das massenhafte Abgreifen von Kommunikationsdaten geschieht innerhalb und teilweise auch außerhalb Großbritanniens an den Glasfaserkabeln. Dass dieser Zugriff durch den Geheimdienst GCHQ stattfindet und die Daten auch massenhaft ausgewertet werden, ist vom britischen Intelligence and Security Committee (ISC) eingeräumt worden und wird auch von der britischen Regierung nicht mehr bestritten. In den Snowden-Papieren befand sich der mittlerweile auch nicht mehr bestrittene Nachweis, dass vom GCHQ eine Operation namens *Tempora*[4] durchgeführt wurde, bei der riesige Datenmengen abgeschnorchelt und durchsucht wurden.

Die Massenüberwachung der Kommunikation an sich bleibt nach dem Urteil prinzipiell weiterhin möglich. Wie schon im ersten Urteil[5] wird sie eben nur beschränkt und eingehegt. Das kann die Beschwerdeführer zwar nur enttäuschen, aber nicht wirklich überraschen. Vielleicht war dafür die Zeit (noch) nicht reif.

Die Begründung des Gerichts

Die erste der Beschwerden (unter dem Motto „Privacy not Prism“[6]) wurde bereits am 29. September 2013 eingereicht und später mit weiteren Verfahren zusammengelegt. Diese breit angelegten Beschwerden liefen also über sieben Jahre.

Es ging darin nicht nur um die breite Überwachung von Kommunikation an sich, sondern auch um die Kontrolle und Aufsicht dieser Praxis und um die Weitergabe von Daten an weitere Geheimdienste. Denn die teilweise nicht öffentlich verfügbaren Regeln, nach denen britische Geheimdienststellen Datensätze aus der Massenüberwachung an Partnergeheimdienste ohne eine richterliche Prüfung weitergeben, oder gar die fehlenden Vorschriften zur Kontrolle und zur Verwendung der Selektoren wa-

ren ebenfalls bemängelt worden. Hierzu finden sich in dem Urteil erhebliche neue Anforderungen, die künftig zu erfüllen sind.

Die Begründung in den Worten des Gerichts (in Absatz 425), warum die britische Massenüberwachung gegen den Artikel 8 der Menschenrechtskonvention verstößt:

> *[…] the Court recalls that there is considerable potential for bulk interception to be abused in a manner adversely affecting the rights of individuals to respect for private life […] Therefore, in a State governed by the rule of law […] section 8(4) regime […] did not contain sufficient „end-to-end" safeguards to provide adequate and effective guarantees against arbitrariness and the risk of abuse. In particular, it has identified the following fundamental deficiencies in the regime: the absence of independent authorisation, the failure to include the categories of selectors in the application for a warrant, and the failure to subject selectors linked to an individual to prior internal authorisation […] These weaknesses concerned not only the interception of the contents of communications but also the interception of related communications data […].*

Der Schutz der Millionen Betroffenen gegen Missbrauch der Daten ist also nicht ausreichend, es existiert keine unabhängige Institution zur Autorisierung der Überwachung und es mangelt dabei auch an einer sinnvollen Kategorisierung bei den Selektoren. Das gilt sowohl für Inhaltsdaten als auch für die Metadaten der Kommunikation.

Wichtige Verbesserungen eingefordert

Die erste Anforderung, die mit dem Urteil der Großen Kammer des Gerichtshofs nun allen Staaten der Konvention auferlegt wurde, betrifft die unabhängige Autorisierung der Massenüberwachung: Ein Richter oder eine andere unabhängige Stelle soll eine aussagekräftige und präzise Ermächtigung erteilen, die einen „Ende-zu-Ende"-Schutz („end-to-end" safeguards) enthält. Der „Ende-zu-Ende"-Schutz bezieht sich auf die verschiedenen Stufen der Datenerfassung und -auswertung, die vom Gericht unterschieden werden. In allen diesen Stufen müssen also künftig Sicherungen gegen Missbrauch vorgesehen werden, beginnend von der ersten Datensammlung über den Einsatz der Selektoren bis zum Speichern in den Datenhalden.

Für Großbritannien wird diese Neuanforderung eine Gesetzesänderung nötig machen, da die Ermächtigung zur Massenüberwachung bisher der Innenminister erteilt. Da der Minister schon keine unabhängige Institution ist, wird der britische Gesetzgeber tätig werden müssen. Aber auch der neue „Ende-zu-Ende"-Schutz in allen Stufen wird allen Staaten, die Massenüberwachung betreiben, zu denken geben müssen – inklusive Deutschland. Das BND-Gesetz[7] muss also auch abgeklopft werden.

Neu ist zudem eine weitere Anforderung, die auch für die Kategorien der Selektoren eine unabhängige Autorisierung vorschreibt. Es kann in Zukunft keine Allgemeinplätze mehr geben, die faktisch der Art der Selektoren keine Grenzen setzen: Einfach nur „nationale Sicherheit" dranschreiben, wird künftig nicht mehr ausreichen. Die Selektoren sind deswegen von besonderer Bedeutung, weil sie letztlich darüber entscheiden, welche Inhalte aus den massenhaften Daten technisch ausgewählt und dann von Analysten wahrgenommen, gelesen oder angehört werden.

Beide Neuerungen bedeuten eine erhebliche Verbesserung für die Menschenrechte von mehr als 820 Millionen Europäern[8], da solche höchstrichterlichen Anforderungen von allen 47 Staaten des Europarats umzusetzen sind.

Neben den beiden wichtigen Verbesserungen – aus Sicht der von Massenüberwachung Betroffenen – gegenüber dem ersten Urteil des Gerichts vom September 2018 betonen die Richter der Großen Kammer die Wichtigkeit des Schutzes von Journalisten. Auch hier muss künftig eine unabhängige Prüfung stattfinden, bevor auf journalistische Quellen zugegriffen werden darf. In seiner Pressemitteilung fasst das Gericht zusammen:

> *The Court also found that the bulk interception regime had breached Article 10, as it had not contained sufficient protections for confidential journalistic material.*

Der Schutz von Journalisten muss also künftig besser berücksichtigt werden.

Viele Jahre lang schlicht illegal

Die juristische Aufarbeitung der Veröffentlichungen aus den Snowden-Papieren kommt mit dem heutigen Urteil in gewisser Weise zu einem Ende. Zwar laufen weitere innerbritische IPT-Verfahren (Investigatory Powers Tribunal)[9], aber keine höchstrichterlichen Verfahren in Europa mehr. In den Vereinigten Staaten wurde die Rechtswidrigkeit der geheimdienstlichen Massenüberwachung von US-Amerikanern im Jahr sieben nach Snowden[10] bereits gerichtlich festgestellt. In Europa haben wir durch den Menschenrechtsgerichtshof nun die unzweifelhafte Feststellung, dass die vormals geheimen britischen Operationen des massenhaften Abgriffs von Kommunikationsdaten nach menschenrechtlichen Standards viele Jahre lang schlicht illegal waren.

Das sollte man erstmal sacken lassen.

Aber ignorieren kann man leider auch nicht: Die Aufmerksamkeit für die Machenschaften der Geheimen ist über die Jahre merklich abgeebbt oder von anderen politischen Problemen überlagert. Dass die Geheimdienste der Five Eyes[11] und weiterer Staaten weiterhin massenweise Daten horten, auswerten und in ihnen schürfen, ist zwar vielen bekannt, aber oftmals kein drängendes Ärgernis mehr.

Das britische GCHQ und die US-amerikanische NSA und mit ihnen weitere Geheimdienste haben seit dem elften September 2001 eine Vielzahl an Überwachungsprogrammen gestartet, sind mit Hunderten Millionen aus dem Säckel der Steuerzahler in den jeweiligen Ländern ausgestattet worden und nutzen die technologische Revolution, die in die Hosentaschen, Büros und Wohnungen der Menschen einzog, auf ihre Weise. Snowden hat uns seltene Einblicke in diese Programme gewährt und

Verfahren wie das mit dem heutigen Urteil beendete erst möglich gemacht.

Aber auch im Rahmen der Schriftsätze und bei den beiden Anhörungen[12] des Gerichtshofs haben die Vertreter der britischen Regierung über die Durchführung der technisierten Massenüberwachung mit sehr wenigen Ausnahmen nur eingeräumt, was nicht mehr abzustreiten war. Wie genau die automatisierten Filterprozesse, die in nahezu Echtzeit über die riesigen Datenmassen laufen, in der Praxis funktionieren, liegt noch immer nur teilweise offen.

Der Massenüberwachung weiterhin die Stirn bieten

Mehr als zweihundert Seiten Text umfasst die Entscheidung, denn rechtlich und technisch ist die Materie komplex. Auch wenn der Schriftsatz mit Sicherheit in den kommenden Tagen noch sehr detailliert analysiert wird, so steht eines fest: Die Massenüberwachung wird mit dem Urteil nicht beendet.

In der Parallelwelt der Geheimdienste, in der eigene Regeln gelten und in der trotz zahlreicher Skandale der politische Schutzschirm noch immer recht sicher war, wird das Urteil dennoch nicht nur Freude hervorrufen. Daran zu rütteln, dass die riesigen Behörden jeden Tag Millionen Datenhäppchen einsammeln und auswerten, dürfte nicht nur in Großbritannien und nicht nur unter Geheimdienstlern aufmerksam verfolgt werden. Denn gegen die Massenüberwachung als solche anzukämpfen, muss auch jene interessieren, die sonst noch an die Datentöpfe wollen: Das sind neben den Geheimen nämlich auch Strafverfolgungsbehörden in den Ländern, in denen die Menschenrechtskonvention gilt. Wenn das Gericht nun also schärfere Regeln vorschreibt, müssen sich alle daran messen lassen.

Es lohnt sich, der Massenüberwachung auch weiterhin die Stirn zu bieten – rechtlich, technisch und politisch. Ein paar mehr Leute vom Schlag eines Snowden könnten wir da übrigens ganz gut gebrauchen.

Quelle: https://netzpolitik.org/2021/snowden-enthuellungen-menschenrechtsgerichtshof-schraenkt-massenueberwachung-der-geheimdienste-ein/

Anmerkungen

1 *https://www.echr.coe.int/Documents/Court_in_brief_ENG.pdf*
2 *Der Beitrag wurde am 25. Mai 2021 veröffentlicht (d. Red.).*
3 *https://hudoc.echr.coe.int/eng#%7B%22documentcollectionid2-%22:[%22GRANDCHAMBER%22,%22CHAMBER%22],%22itemid%22:[%22001-210077%22]%7D*
4 *https://netzpolitik.org/2013/tempora-neue-snowden-dokumente-nennen-weitere-von-grossbritannien-angezapften-glasfaser-kabel-auch-deutsche/*
5 *https://netzpolitik.org/2018/nach-dem-urteil-die-europaeische-menschenrechtskonvention-auf-den-stand-der-digitalen-revolution-bringen/*
6 *https://netzpolitik.org/2019/wieder-vor-gericht-geheimdienstliche-massenueberwachung-und-das-menschenrecht-auf-privatheit/*
7 *https://netzpolitik.org/2020/zugestaendnisse-die-keine-sind/*
8 *https://de.wikipedia.org/wiki/Europarat*
9 *https://www.ipt-uk.com/content.asp?id=11?id=11*
10 *https://www.reuters.com/article/us-usa-nsa-spying/u-s-court-mass-surveillance-program-exposed-by-snowden-was-illegal-idUSKBN25T3CK*
11 *https://de.wikipedia.org/wiki/Globale_Überwachungs-_und_Spionageaffäre#Five_Eyes_(UKUSA)*
12 *https://netzpolitik.org/2019/massenueberwachung-der-kommunikation-anhoerung-beim-menschenrechtsgerichtshof/*
13 *https://de.wikipedia.org/wiki/Constanze_Kurz*
14 *https://nowyouknow.eu/*
15 *http://gewissensbits.gi.de/constanze-kurz/*
16 *https://www.randomhouse.de/Buch/Cyberwar-Die-Gefahr-aus-dem-Netz/Constanze-Kurz/C.-Bertelsmann/e537921.rhd*
17 *http://www.faz.net/aktuell/feuilleton/aus-dem-maschinenraum/*
18 *https://www.privacynotprism.org.uk/*
19 *https://www.youtube.com/watch?v=hj3gAsqrB18*
20 *https://de.wikipedia.org/wiki/Werner_Holtfort#Holtfort-Stiftung*
21 *https://media.ccc.de/search?q=Constanze+Kurz*
22 *http://www.ev-akademie-tutzing.de/toleranz-preis-fuer-christian-wulff-und-constanze-kurz/*
23 *https://www.jungundnaiv.de/2020/05/03/constanze-kurz-ueber-die-corona-app-folge-460/*
24 *https://pgp.mit.edu/pks/lookup?op=get&search=0x4A13B8EE269F8A45*

Constanze Kurz

Constanze Kurz[13] ist promovierte Informatikerin, Autorin und Herausgeberin[14] von mehreren Büchern[15], zuletzt zum Cyberwar[16]. Ihre Kolumne *Aus dem Maschinenraum*[17] erschien von 2010 bis 2019 im Feuilleton der *FAZ*. Sie ist Aktivistin[18] und ehrenamtlich Sprecherin[19] des *Chaos Computer Clubs*. Sie forschte an der Humboldt-Universität zu Berlin am Lehrstuhl „Informatik in Bildung und Gesellschaft" und war Sachverständige der Enquête-Kommission *Internet und digitale Gesellschaft* des Bundestags. Sie erhielt den *Werner-Holtfort-Preis*[20] für bürger- und menschenrechtliches Engagement[21], den Toleranz-Preis[22] für Zivilcourage und die Theodor-Heuss-Medaille für vorbildliches demokratisches[23] Verhalten.
Kontakt: *constanze(at)netzpolitik.org* (PGP[24]).

Stefan Hügel

BigBrotherAwards 2021

Auch im letzten Jahr gab es wieder reichlich Ereignisse, die einen BigBrotherAward verdient hätten. Wie immer berichten wir von der Preisverleihung: Wer hat es in den erlesenen Kreis der Preisträger:innen geschafft?

Wir fassen in diesem einleitenden Beitrag des Schwerpunkts zum BigBrotherAward 2021[1] zunächst die Laudationes für die PreisträgerInnen kurz zusammen. Danach drucken wir zwei Laudationes im Wortlaut ab. Die Verleihung fand am 11. Juni 2021 in der *Hechelei* in Bielefeld statt.

Eine Besonderheit in diesem Jahr war der Abschied von Rolf Gössner aus der Jury. In einer Rede hielt er Rückschau auf seine Mitarbeit in der Jury und seine Laudationes auf Preisträger:innen in zwanzig Jahren.[2] Seine Laudationes waren immer ein Höhepunkt der Verleihungen – sie sind jetzt auch in Buchform erhältlich (siehe Verlagsankündigung auf Seite 79/80).

Kategorie *Verkehr*

Der BigBrotherAward in der Kategorie *Verkehr* ging an die **Europäische Kommission**,

für die Einführung des On-Board Fuel Consumption Meter (OBFCM) im Rahmen der EU-Verordnung 2019/631.

Laudator Frank Rosengart erläuterte:

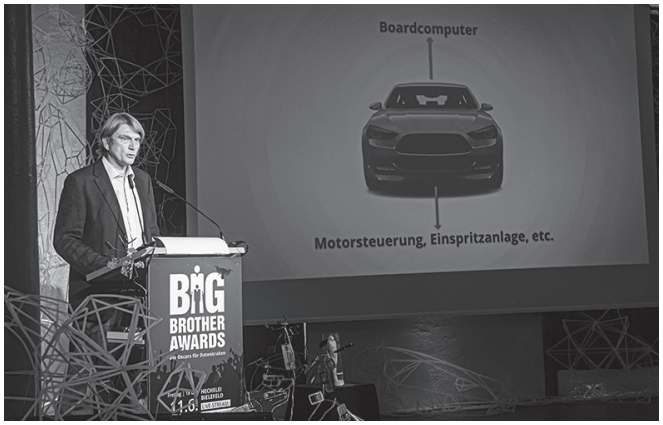
> *„Für die EU ist es wichtig, realistische Verbrauchsdaten zu ermitteln, da den Herstellern eine Obergrenze des CO_2-Ausstoßes für Neuwagen auferlegt wurde. Bei Überschreitung werden Strafen fällig. Außerdem sollen potentielle Autokäufer:innen eine Idee bekommen, was ihr Wunschauto tatsächlich verbraucht, und nicht nur schöngerechnete Werte. Deshalb sollen die Verbrauchswerte nicht nur im Labor, sondern an den tatsächlich gefahrenen Autos ermittelt werden."*

Da nun ohnehin alle Motordaten während des Betriebs eines Fahrzeugs durch den Bordcomputer erfasst werden und die Fahrzeuge dank des e-Call auch über ein Mobilfunkmodul verfügen, können diese dann auch laufend an eine entsprechende Stelle übermittelt werden. Durch die Echtzeitübermittlung will man verhindern, dass Laborwerte geschönt und dann erst bereitgestellt werden.

Mit der Übermittlung sollen die Hersteller selbst beauftragt werden. Sie sollen mit der Fahrzeug-Identifikationsnummer laufend die Verbrauchswerte, gefahrene Kilometer und bei Bedarf weitere (in der Verordnung nicht weiter spezifizierte) Parameter übermitteln. Damit kommen auch die Hersteller selbst in den Besitz der Daten, auf die sie sonst nur mit ausdrücklicher Einwilligung des Fahrzeughalters Zugriff hätten. Im Rahmen einer Initiative *Datenraum Mobilität* plant auch die Bundesregierung, einen Datenpool solcher Fahrzeugdaten einzurichten.

> *„Mit der elektronischen Verbrauchsdatenerfassung und -übermittlung (die englische Abkürzung dieses Verfahrens ist „OBFCM") wird ein weiteres Mosaiksteinchen in Richtung gläserne Autofahrer:innen gelegt, obwohl dies gar nicht notwendig wäre. Wir sehen mit Sorge, wie Telematikdienste ihren Weg in die Autos finden und der Datenschutz dabei auf der Strecke bleibt",*

stellt Frank Rosengart abschließend fest.



Frank Rosengart – Foto: Matthias Hornung CC BY-SA 4.0

Kategorie *Bildung*

Peter Wedde hielt die Laudatio in der Kategorie *Bildung*. Dieser Preis ging an die **Proctorio GmbH in München-Unterföhring**,

für die ebenfalls Proctorio genannte KI-basierte Prüfungssoftware.

Er erläutert dazu einleitend den Hintergrund:

> *„Der Name Proctorio leitet sich aus dem englischen Wort Proctoring ab, das sich mit* beaufsichtigen *übersetzen lässt. Proctorio geht es um ‚Online-Proctoring', das heißt um die Beaufsichtigung von Prüflingen im Hochschulbereich per Internet.*
>
> *Mit Blick auf dieses Geschäftsmodell war der Ausbruch der Corona-Pandemie Anfang 2020 für die Firma aus Marketingsicht ein absoluter Glücksfall: Lehrende mussten aufgrund umfassender Lockdown-Maßnahmen und ‚Shutdowns' geplante Präsenzprüfungen von einem Tag auf den anderen einstellen. Anreisen zu Klausuren mit öffentlichen Verkehrsmitteln stellten ebenso eine Gesundheitsgefahr dar wie der stundenlange Aufenthalt in einem Hörsaal. Studierende machten sich berechtigte Sorgen um die Fortsetzung oder um den Abschluss ihres Studiums."*

Die Firma Proctorio bietet ein Produkt an, mit dem die „vollautomatische und sichere Prüfungsaufsicht für Online-Prüfungen" ohne direkte Anwesenheit eines menschlichen Prüfers möglich sein soll, z. B. beim Prüfling zu Hause, auf dem eigenen Rechner.

Aber, wie Peter Wedde weiter erläutert:

> *„Die Software Proctorio greift tief in die Integrität der privaten Geräte der Studierenden ein. Um an Prüfungen teilnehmen zu können, müssen sie die Software auf ihren Computern installieren und Proctorio für die Dauer einer Prüfung die Kontrolle über ihr Gerät überlassen."*

Die Software ermöglicht es, bestimmte Aktionen auf dem Rechner zu sperren, etwa Downloads während der Prüfung. Prüfer:innen können zu Beginn der Prüfung verlangen, ihnen den Raum über die Videokamera vorzuführen. Sie können dann Studierende während der Prüfung beobachten. Die Software bietet aber auch eine automatisierte Überwachung an, indem die Videosignale mit Künstlicher Intelligenz ausgewertet werden und damit überprüft wird, ob sich beispielsweise eine weitere Person im Raum befindet. Vermehrte Blicke in eine bestimmte Richtung werden als verdächtig markiert. Videoaufzeichnungen mit Auffälligkeiten können durch die Prüfer:innen kontrolliert werden. Das Risiko einer Fehlbeurteilung tragen die geprüften Studierenden.

Peter Wedde abschließend:

> *„Wir halten fest:*
>
> - *Die Nutzung von Proctorio für die Beaufsichtigung von Online-Prüfungen führt zu einem schweren Eingriff in die Integrität der privaten Geräte der Studierenden.*
> - *Die permanente Videoüberwachung der Prüflinge während der Prüfungszeit ist ein schwerer Eingriff in ihre Privatsphäre und in ihre privaten Räume – insbesondere, wenn ein Raum-Scan stattfindet.*
> - *Die von ‚KI'-Software durchgeführten automatischen Analysen ihres Verhaltens sind für die betroffenen Studierenden nicht transparent. Die allgemeine Unschuldsvermutung, die für alle Bürger gilt, wird durch die verwendeten Algorithmen und die hieraus folgende intransparente Kontrolle außer Kraft gesetzt.*
> - *Die Gestik und insbesondere Augenbewegungen werden permanent erfasst und ausgewertet. Die Software kann hieraus negative Schlussfolgerungen ziehen, was den Druck und den Stressfaktor für die Studierenden erhöht.*
> - *Online-Prüfungen zu Hause finden manche Studierende sicher angenehm. Sie gefährden aber aufgrund ungleicher Wohn- und Lebensverhältnisse die Chancengleichheit, die bei der Ablegung von ‚Präsenzprüfungen' hergestellt werden soll.*
> - *Das Einsparpotential, das Proctorio für automatisierte Prüfungsaufsichten verspricht, macht die Software für kostenbewusste Hochschulen attraktiv. Diese Einsparung geht aber auf Kosten der Studierenden, die mit klassischen Präsenzprüfungen besser zurecht kommen als mit Online-Prüfungen unter den Augen einer Software.*
> - *Die Datenschutzkonformität ist schon deshalb zweifelhaft, weil belastbare Aussagen zur Rechtsgrundlage fehlen und eine ‚freiwillige Zustimmung' der Studierenden in Prüfungssituationen wohl eher nicht gewährleistet ist.*
>
> *Gründe genug für den BigBrotherAward in der Kategorie Bildung.*

Peter Wedde – Foto: Matthias Hornung CC BY-SA 4.0

Kategorie *Public Intellectual*

Der BigBrotherAward in der Kategorie *Public Intellectual* wurde an den Philosophen und stellvertretenden Vorsitzenden des Deutschen Ethikrats, Professor Dr. **Julian Nida-Rümelin** verliehen. Er erhielt den Preis

für seine öffentlich mehrfach geäußerte unhaltbare Behauptung, dass „der Datenschutz" die Bekämpfung von Corona erschwert und Tausende von Toten zu verantworten habe.

Laudator padeluun kritisiert:

> *„Er sagte und wiederholte die Ansicht, dass … ‚in Deutschland der Datenschutz eine vernünftige Warn-App verhindere. Anders als in Südkorea, wo man die Pandemie mit Apps ohne Datenschutz super in den Griff bekommen habe'."*

Die vollständige Laudatio, in der padeluun die Preisvergabe erläutert, ist ab Seite 61 nachzulesen. Sein Fazit:

> *Viele haben in dieser verfluchten Corona-Pandemie mit den notwendigen Einschränkungen von Freizügigkeit und existenzbedrohenden finanziellen Verlusten hier und da Dinge von sich gegeben, die man bei klarem Verstand so nicht gesagt hätte. All denen gegenüber müssen wir Barmherzigkeit walten lassen. Den Schauspielern, die sich jetzt für ihre komische Aktion schämen. Und den Leuten, die als Querdenker:innen ein paar gewissenlose Hetz-Trolle reich gemacht haben. Und die dabei nicht gemerkt haben, dass der Gebrauch ihres eigenen Verstandes eine Zeitlang in die Irre geführt hat. Ihnen allen – auch Herrn Nida-Rümelin – möchte ich zurufen: Wer A sagt, muss nicht immer wieder A sagen. Man kann auch erkennen, dass A falsch war.*

Kategorie *Was mich wirklich wütend macht*

Der BigBrotherAward in der Kategorie *Was mich wirklich wütend macht* wurde von Rena Tangens angekündigt. Er wurde verliehen

für Manipulationen des Werbemarktes auf Kosten von Content-Schöpfer:innen sowie Enteignung von User-Verhaltensdaten.

Sie leitete die Preisvergabe – die letzlich an **Google** ging – in ihrer Laudatio ausführlich her. Zunächst erläutert sie den Hintergrund:

> *„Cookiebanner! Diese Pest! Sie kennen das: Sie rufen eine Webseite auf und – zack! – schon schiebt sich dieser Kasten mit unsäglich schlechtem Design über das, was Sie eigentlich sehen wollen. Dann müssen Sie sich entscheiden: Wollen Sie einfach nur schnell an die gewünschte Webseite, dann klicken Sie einfach auf den großen bunten Button* Okay. *Doch wenn Sie das mit Ihren Rechten ernst nehmen, dann wird es kompliziert. Augen zusammenkneifen, kleine graue Schrift auf weißem Grund lesen, und minutenlang alles einzeln wegklicken, was Sie nicht wollen. Und das ist verdammt viel: bis zu 470 Tracker zum Beispiel alleine bei der Süddeutschen Zeitung. ‚Will ich alles nicht!' wird Ihnen gar nicht erst angeboten. Und wenn Sie alle Tracker einzeln in mühsamer Handarbeit weggeklickt haben, dann passen Sie bloß auf, denn der nächste freundlich-bunte Button heißt* Alles zulassen *und nicht* Meine Auswahl abspeichern. *Der ist grau. Aber Vorsicht – auch da sollten Sie nicht draufklicken. Denn vorher müssen Sie noch die meist gut verborgene Kategorie* Berechtigtes Interesse *finden. Dort steht nämlich auch alles auf aktiviert, und Sie müssen es wegklicken. Haben Sie's gewusst?"*

Die vollständige Laudatio von Rena Tangens ist ab Seite 63 nachzulesen.

Kategorie *Gesundheit*

Den letzten BigBrotherAward gab es an diesem Abend in der Kategorie *Gesundheit*. Er ging an die Firma **Doctolib** in Berlin

für ihr Terminvermittlungsportal für Ärzte.

Laudator Thilo Weichert begründete die Verleihung:

> *„Doctolib verarbeitet mit diesem Portal unter Missachtung der ärztlichen Vertraulichkeit die Daten von zigtausenden Patient:innen.*
>
> *Das Angebot für Gesundheitsfachkräfte, also vor allem für Ärzte, und deren Patienten, ist genial: Die Ärzte schließen einen Vertrag mit Doctolib ab, erteilen Zugriff auf ihre Patientendaten und können dann über eine Internetseite Behandlungs-, Beratungs- oder Impftermine verbindlich verabreden lassen. Und schon können die Patient:innen online Termine buchen. Kein Warten in einer Telefonwarteschleife, keine gestressten Mitarbeiter:innen, selbst das Erinnern der Patient:innen an den Termin übernimmt Doctolib – und für das alles zahlen die Praxen nur etwas mehr als 100 € im Monat. …"*

Um diese Dienstleistung erbringen zu können, benötigt Doclib zunächst den gesamten Patientenstammdatensatz, der auch später regelmäßig abgeglichen werden muss. Diese Daten werden im Rahmen einer Auftragsdatenverarbeitung weiter verarbeitet. Dabei werden die Daten in den eigenen Datenbanken von Doclib zur Terminvergabe zusammengeführt – die Weiternutzung ist unklar.

Gesundheitsdaten sind besonders sensible Daten und werden durch die Datenschutz-Grundverordnung besonders geschützt. Ärzt:innen dürfen für diese Daten Auftragsdatenverarbeitungsverträge ohne explizite Zustimmung der Patient:innen abschließen. Problematisch wird es, wenn ohne Information der Betroffenen Daten von Patient:innen weitergegeben werden, die keine Termine vereinbaren und kein Konto bei Doctolib haben. Die Daten der Patient:innen dürfen an technische Dienstleister weitergegeben werden, wenn sie für den Dienst erforderlich sind. Der Import der gesamten Patientenliste eine:r Ärzt:in ist aus Sicht von Thilo Weichert definitiv nicht erforderlich. Grundsätzlich gilt auch die Mandantentrennung, d. h. die Patientendaten verschiedener Ärzt:innen dürfen nicht zusammengeführt werden.

Und so schließt Thilo Weichert seine Laudatio:

> *„Die Digitalisierung unseres Gesundheitssystems ist wichtig, um die Gesundheitsversorgung der Bevölkerung zu verbessern und auf einem hohen Niveau zu halten. Dies darf aber nicht auf Kosten der Vertraulichkeit zwischen Patient:innen und Heilberufen passieren. Dafür, dass Doctolib diese Vertraulichkeit seinem Expansionsstreben unterordnet, dafür erhält das Unternehmen den BigBrotherAward 2021 in der Kategorie Gesundheit."*

Anmerkungen

1 *Weitere Informationen und Nachweise finden sich auf der Webseite der BigBrotherAwards, http://www.bigbrotherawards.de. Von dort stammen auch alle Zitate aus den Laudationes.*

2 *Rolf Gössner (2021) Datenkraken im öffentlichen Dienst. „Laudatio" auf den präventiven Sicherheits- und Überwachungsstaat. Köln: Papyrossa; ausführliche Ankündigung in dieser Ausgabe der FIfF-Kommunikation auf Seite 79*

Dr. Thilo Weichert – Foto: Matthias Hornung, CC BY-SA 4.0

Kategorie *Public Intellectual* – Laudatio

Der BigBrotherAward 2021 in der Kategorie Public Intellectual geht an den Philosophen und stellvertretenden Vorsitzenden des Deutschen Ethikrats, Prof. Dr. phil. Dr. h. c. Julian Nida-Rümelin,

für seine öffentlich mehrfach geäußerte unhaltbare Behauptung, dass „der Datenschutz" die Bekämpfung von Corona erschwert und Tausende von Toten zu verantworten habe.

Natürlich benötigen die Missklänge um die Corona-Pandemiebekämpfung einen Widerhall bei den BigBrotherAwards. Und ich habe lange gebraucht, um zu entscheiden, welchen Namen ich hier als Preisträgerin oder Preisträger nennen möchte. Über Coronapolitik, Sinn und Unsinn gibt es eine Menge zu sagen – was leider auch viele tun. Da komme ich auch noch zu.

Aber erst einmal meine Begründung, warum ich über Herrn Nida-Rümelin wirklich erzürnt bin.

Er sagte und wiederholte die Ansicht, dass (ich fasse da mal zusammen) „in Deutschland der Datenschutz eine vernünftige Warn-App verhindere. Anders als in Südkorea, wo man die Pandemie mit Apps ohne Datenschutz super in den Griff bekommen habe".

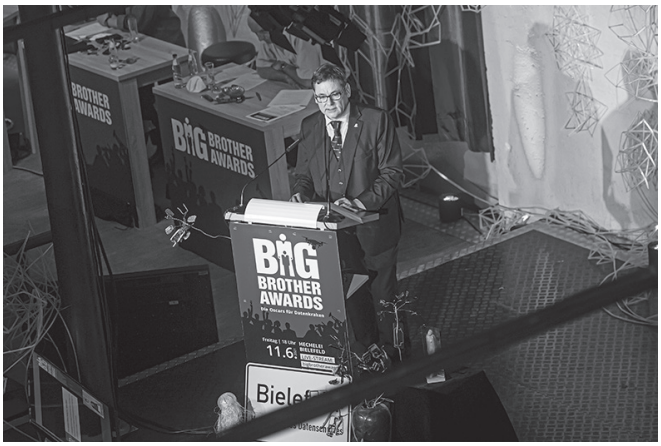
Der Journalist Markus Beckedahl bezeichnete diese Sichtweise als *Talkshow-Mythos*.[1] Demnach wird die App in Südkorea nämlich vor allem dazu eingesetzt, um die Quarantänebestimmungen einzuhalten, weniger dazu, um Infektionsketten nachzuverfolgen und zu unterbrechen. Und der Blogger Linus Neumann, der hier an dieser Stelle auch schon einmal eine Laudatio gehalten hat, ergänzt[2]: „Die südkoreanische App hatte Ende Juli ein schweres Datenleck und Südkorea kämpft gerade mit der zweiten Welle. Einen Ausbruch im August hat Korea hingegen unter Kontrolle gebracht – mit einem Lockdown. Auch dieser ‚Erfolg' kann also nicht als argumentative Grundlage dienen für das, was Nida-Rümelin behauptet."

Auch sonstige Behauptungen Nida-Rümelins zerpflückt Linus Neumann genüsslich in seinem Blog.[3]

Was treibt einen anscheinend klugen Mann wie Nida-Rümelin dazu, sich im Fernsehen, Radiosendungen, in Zeitungen dazu auszulassen, dass der Datenschutz „Tausende Corona-Tote zu verantworten hätte"? Wie klein muss sein großer Geist sein, damit der ihm nicht noch mal eine Warnung zuflüstert, bevor er so eine offensichtliche Dummheit in die Welt hinausruft?

Herr Nida-Rümelin ist Philosoph, Politiker, ehemaliger Kulturstaatsminister, stellvertretender Vorsitzender der Ethikrats. Dortselbst ist er Presseansprechpartner für Digitalisierung.

Schon im Mai letzten Jahres ließ er sich auf SWR1[4] aus. Im September 2020 haben wir das für die BigBrotherAwards noch ignoriert. „Don't make stupid views famous." Leider hat der Denker Nida-Rümelin diese Chance nicht zum Denken genutzt. Bei der Unterhaltungssendung „Anne Will"[5] im Dezember 2020 wiederholte er seine falschen Parolen gegen den Datenschutz.



Laudator padeluun – Foto: Matthias Hornung CC BY-SA 4.0

Und dann, im März 2021 – da waren alle Fakten, auf die er sich gestützt hatte, längst komplett widerlegt – verbreitete er seine alternativen Meinungen erneut, diesmal über die Deutsche Presseagentur. Da dachte ich dann wirklich: Ach, Philosoph, hättest Du doch geschwiegen …

Nein, Julian Nida-Rümelin und Ihr anderen „Anti-Datenschutz"-Apologeten: Datenschutz tötet nicht. Datenschutz ist die dünne Membran, die uns alle vor der Barbarei staatlicher und kommerzieller Übergriffigkeiten schützt.

Datenschutz, beziehungsweise ‚Informationelle Selbstbestimmung', beziehungsweise „Menschenschutz", vom Bundesverfassungsgericht 1983 aus den ersten zwei Absätzen des Grundgesetzes abgeleitet, seit der Inkraftsetzung der Datenschutzgrundverordnung ein weltweiter Innovationsmotor, ist ein Thema, das wie kein anderes das geschulte philosophische Denken fordert, weil diese verdammte digital vernetzte Welt nun mal nicht mit Hämmern und Nägeln vergleichbar und nicht mit mechanischen Modellen darstellbar ist.

Wir haben in den vergangenen 4 Jahrzehnten die Darstellung unserer Welt und unsere Kommunikation darüber in Nullen und Einsen zerlegt. Es sind Stromschwankungen, die potenziell gleichzeitig an Millionen und Milliarden Orten bis hinein in den erdnahen Orbit und das Universum gleichzeitig kopiert werden – völlig ohne dass das an der Ursprungsstelle erfahrbar ist.

Was das fürs Menschsein bedeutet, haben Sie, Herr Nida-Rümelin – genauso wie die anderen Schwachmaten, die zurzeit ein digitales Pro-Terrorgesetz nach dem anderen verabschieden – noch lange nicht durchdrungen. Darüber muss man nachdenken, bevor man den Erwachsenen reinredet. Da muss man zuhören, wenn die Erwachsenen drüber reden. Da muss man seinen Verstand gebrauchen, wenn man der Gesellschaft weiter helfen will.

(Ich bitte die Arroganz der vorstehenden Sätze zu entschuldigen: Sie sind meiner Verzweiflung geschuldet.)

Digitaler Menschen- und Gesellschaftsschutz braucht Präzision.

Ja, ich benenne das Wort Datenschutz jetzt mal zum besseren Verständnis um. Denn Datenschutz bedeutet nicht, dass Daten geschützt werden müssen – das wäre Datensicherheit – sondern, dass Menschen und Gesellschaft Schutz brauchen.

Also nochmal: Digitaler Menschen- und Gesellschaftsschutz braucht Präzision.

Digitaler Menschen- und Gesellschaftsschutz braucht geschultes Denken.

Digitaler Menschen- und Gesellschaftsschutz braucht Philosophie.

Das denkt sich nun mal nicht so schnell zwischen Häppchen und Interview.

Ich erwarte von einem studierten und lehrenden Philosophen, dass er nicht einfach wie jeder andere dahergelaufene Verschwörungsheini undurchdachten Blödsinn in die Welt hinausbläst. Oder erwarte ich da einfach zu viel? Hat mir mein gefährliches Halbwissen von Platons Traum der „Philosophenherrschaft“ schon selbst den Verstand vernebelt, so dass ich jetzt enttäuscht bin über meine Vorstellung von einer Denk-Elite, die nicht mehr als ungare Plattitüden 'raushaut?

Ich möchte hier auf gar keinen Fall einer keimenden Intellektuellenfeindlichkeit das Wort reden. Im Gegenteil.

Natürlich gehört es zum Beruf eines Philosophen, steile Thesen zu proklamieren – aber es gehört auch dazu, sich dem Diskurs zu stellen und diese Thesen prüfen und angreifen zu lassen, und aus dem Diskurs zu lernen. Und das Gelernte muss dann anschließend in neue Thesen eingebaut werden. Und dann, wenn man in vielen nervigen und beflügelnden Diskursen Festigkeit in seiner These erlangt hat, dann erst strebt man zu der großen Bühne und gibt das in die Gesellschaft, was die Gesellschaft als Gesamtes weiterbringt. Man wiederholt auf der großen Bühne nicht ein Jahr lang dumme Behauptungen – und schon gar nicht, wenn deren Faktenbasis inzwischen Stück für Stück komplett widerlegt worden ist.

Wumms.

Und jetzt frage ich mich, was mich selbst denn so von Herrn Nida-Rümelin unterscheidet (abgesehen davon, dass ich meinen Beruf als Künstler bezeichne). Ich stelle mich auch auf mehr oder weniger große Bühnen und postuliere Erkenntnisse. Aber auch, wenn ich das nicht wahrhaben will, bin ich auch nur ein älterer Herr, der ab und an ganz schön sauer ist und durchaus das Mitteilungsbedürfnis hat, andere an dieser Mißstimmung – mit dem Ziel der Verbesserung – teilhaben zu lassen.

Wenn ich mich in der Corona-Diskussion umgucke, sehe ich eine Kakophonie von vielen Herren und ein paar Damen, die einem ihre Erkenntnisse und Ansichten mit Kraft der von ihnen genutzten Medien um die Ohren hauen möchten. Schulen auf? Ja! Schulen zu? Ja! Lockdown? Ist doch gar kein Lockdown! Alles zumachen! Alles aufmachen? Spahn macht alles falsch! Datenschutz stinkt! Die Luca-App ist Betrug! Du genderst falsch! IP-Nummern sind keine personenbeziehbaren Daten! Doch, sind sie! Corona ist eine Absprache des World Economic Forums. Die wollen nur ID2020 durchbringen. Und Billionen über Impfungen einsacken. Putin ist ein lupenreiner Demokrat. Versammlungen sind grundsätzlich verboten. Das war doch nur satirisch gemeint!

In dieser Kakophonie hat Julian Nida-Rümelin als Denker mitgemacht. Und um es ganz schlicht auszudrücken: Er war nicht hilfreich.

Sollte ich Mitleid mit ihm haben, Verständnis zeigen? Ich kann es mal versuchen. Da stehen wir armen Toren, und ohne, dass es blitzt und donnert oder Asche regnet, bricht da eine Pandemie aus. Wir können sie nicht riechen, nicht schmecken. Wir können uns nicht in Feuersbrünste werfen und heldenhaft Frauen und Kinder retten. Wir sind dazu verdonnert, zur Seite zu gehen und Fachleute machen zu lassen.

Er und ich sind keine Pandemiefachleute.

Deshalb interessiert sich auch niemand für uns. Wir sind gar nicht gefragt. Das einzige, was ich Leuten hätte sagen können, war: Ich habe wissenschaftlich arbeitende Menschen in meinem Freundeskreis, die können Statistik verstehen und die sagten mir zu Beginn der Pandemie: Bunker Dich erst mal ein. Zumindest, bis weitere Informationen da sind.

Und dann hat man ein bisschen Zeit, um das Seuchenschutzgesetz zu lesen. Dann versteht man den gesetzlichen Auftrag des RKI. Versteht plötzlich den Unterschied zwischen Katastrophen- und Bürgerschutz. Man weiß dann, dass Seuchenschutz Länderrecht ist. Und dann entdeckt man, dass die Gesundheitsämter überhaupt nicht für die Bewältigung einer Pandemie aufgestellt sind. Dass in den vielen Jahren Gesetzgebung nichts getan wurde, um einer Pandemie zu begegnen. Aber es wurde ein schwachsinniges Gesetz nach dem anderen für den Fetisch „für mehr Sicherheit“ gemacht. In den Gesundheitsämtern sitzen sie mit Papier und Bleistift, Faxgeräten und Wählscheibentelefonen und schaffen es nicht, die Informationsmengen und Anforderungen, die auf sie einstürmen, zu bewältigen. Hier blicken wir auf mindestens 30 Jahre Staatsversagen. Und dann kam noch der Kanzlerkandidatsmachtkampf der CDU dazu, der nicht hilfreich war. Weil unter dem Eindruck dieses Machtkampfes nie klar war, welche Maßnahme wirklich sinnvoll war und welche nur den Gockeleien geschuldet war …

Aber der Datenschutz ist schuld? Ja?! Echt mal!

Ich weiß nicht, ob jemand hier im Raum mal auf einer „Corona-Leugner“-Demo war. Ich war es. Ich habe meinen Presseausweis eingesteckt, meinen Mundschutz aufgesetzt, und ich habe dort mit vielen Leuten gesprochen. Menschen, wie du und ich. Menschen, bei denen ich mir auch vorstellen konnte, dass sie auf einer unserer Demos mitlaufen könnten. Aber auch Menschen, denen geistige Führung fehlt, um eigenständig sein zu können. Die durch das, von dem sie denken, dass es Korruption sei, dieses Haudrauf-Gesetzemachen ohne Sinn und Verstand,

so verunsichert sind, dass sie zu der nächstbesten wohlfeilen Erklärungsalternative greifen.

Ich kann es ihnen nicht wirklich verdenken. Zumal immer mehr Verwirrprofis Morgenluft wittern und nicht nur die dummen Klugen, sondern nun auch die bösen Schlauen mitspielen im Verwirrspiel. Die Leute da sind (mal von den komplett Verstrahlten abgesehen) wirklich überzeugt von ihren Einstellungen, von ihren Zweifeln und den ‚alternativen' Informationen, die sie sich einverleibt haben. Das sind die Menschen, die von denen, die fürs Denken bezahlt werden, allein gelassen worden sind. Nicht nur allein gelassen: Sie wurden dem strukturellen Populismus[6] der sozialen Hetzwerke ausgeliefert. Allein gelassen nicht nur von Herrn Nida-Rümelin, sondern auch von den anderen Herren (und Damen) seines Kalibers.

Deshalb haben wir auch die Kategorie *Public Intellectual* eingeführt – weil wir eigentlich so dringend Menschen brauchen, die denken können und anderen damit Wege weisen. Wie bitter, wenn Menschen wie Herr Nida-Rümelin diesen Auftrag so schändlich für billigen Populismus verraten.

Viele haben in dieser verfluchten Corona-Pandemie mit den notwendigen Einschränkungen von Freizügigkeit und existenzbedrohenden finanziellen Verlusten hier und da Dinge von sich gegeben, die man bei klarem Verstand so nicht gesagt hätte. All denen gegenüber müssen wir Barmherzigkeit walten lassen. Den Schauspielern, die sich jetzt für ihre komische Aktion schämen. Und den Leuten, die als Querdenker:innen ein paar gewissenlose Hetz-Trolle reich gemacht haben. Und die dabei nicht gemerkt haben, dass der Gebrauch ihres eigenen Verstandes eine Zeitlang in die Irre geführt hat. Ihnen allen – auch Herrn Nida-Rümelin – möchte ich zurufen: Wer A sagt, muss nicht immer wieder A sagen. Man kann auch erkennen, dass A falsch war.

In diesem Sinne: Herzlichen Glückwunsch, Julian Nida-Rümelin, zum BigBrotherAward 2021.

Anmerkungen

1 *Quelle: https://www.br.de/nachrichten/netzwelt/hemmt-der-datenschutz-die-pandemie-bekaempfung,SJQ2001*
2 *Quelle: https://linus-neumann.de/2020/12/corona-und-datenschutz-julian-nida-rumelin-verdreht-noch-mehr-tatsachen-als-ich-zunachst-dachte/*
3 *Quelle: https://linus-neumann.de/2020/12/corona-und-datenschutz-julian-nida-rumelin-verdreht-noch-mehr-tatsachen-als-ich-zunachst-dachte/*
4 *Quelle: https://www.ardmediathek.de/video/swr1-leute/prof-julian-nida-ruemelin-oder-philosoph-und-ex-politiker-oder-fordert-eine-andere-strategie-fuer-die-corona-krise/swr-de/Y3JpZDovL3N3ci5kZS9hZXgvbzEyNDE1Njk/*
5 *Quelle: https://daserste.ndr.de/annewill/videos/Lockdown-vor-Weihnachten-schafft-Deutschland-so-die-Pandemie-Wende,annewill6792.html*
6 *Quelle: Joseph Vogl in der Frankfurter Allgemeinen Sonntagszeitung https://www.faz.net/aktuell/feuilleton/debatten/plattformkapitalismus-joseph-vogl-ueber-kapital-und-ressentiment-17241098.html*

Rena Tangens

Kategorie *Was mich wirklich wütend macht*

Die Kategorie für diesen BigBrotherAward ist neu.

Sie heißt: „Was mich wirklich wütend macht!"

Und der diesjährige Preis geht an … – ja, an wen eigentlich?

Das ist diesmal nicht so einfach. Werden Sie gleich sehen.

Also: Was mich wirklich wütend macht

Cookiebanner! Diese Pest! Sie kennen das: Sie rufen eine Webseite auf und – zack! – schon schiebt sich dieser Kasten mit unsäglich schlechtem Design über das, was Sie eigentlich sehen wollen. Dann müssen Sie sich entscheiden: Wollen Sie einfach nur schnell an die gewünschte Webseite, dann klicken Sie einfach auf den großen bunten Button *Okay*. Doch wenn Sie das mit Ihren Rechten ernst nehmen, dann wird es kompliziert. Augen zusammenkneifen, kleine graue Schrift auf weißem Grund lesen, und minutenlang alles einzeln wegklicken, was Sie nicht wollen. Und das ist verdammt viel: bis zu 470 Tracker zum Beispiel alleine bei der Süddeutschen Zeitung. „Will ich alles nicht!" wird Ihnen gar nicht erst angeboten. Und wenn Sie alle Tracker einzeln in mühsamer Handarbeit weggeklickt haben, dann passen Sie bloß auf, denn der nächste freundlich-bunte Button heißt *Alles zulassen* und nicht Meine Auswahl abspeichern. Der ist grau. Aber Vorsicht – auch da sollten Sie nicht draufklicken. Denn vorher müssen Sie noch die meist gut verborgene Kategorie *Berechtigtes Interesse* finden. Dort steht nämlich auch alles auf *aktiviert*, und Sie müssen es wegklicken. Haben Sie's gewusst?

Was mich daran wirklich wütend macht

Diese Cookie-Dialoge sind nach den neuesten Erkenntnissen über menschliche Wahrnehmung, Psychologie und Webdesign für ergonomisch ansprechende Webseiten gestaltet. Also:

- Wichtige Handlungsoptionen werden im Fließtext versteckt, während das *OK* auf einem fetten Button thront.
- Sie werden in unlesbaren Farben und Schriftgrößen angezeigt.
- Der *Alles-zulassen*-Button steht unten rechts – wo wir eigentlich die Bestätigung unserer Auswahl erwarten.

- Bei vielen Schaltern ist die rechts-links-Position vertauscht: Wenn ich dort klicke, wo ich vorher Tracker deaktiviert habe, werden mit dem Zentral-Schalter plötzlich alle wieder aktiviert.

- Und dann gibt es noch sprachliche Ungetüme, komplizierte Formulierungen und mehrfache Verneinungen, um uns maximal zu verwirren.

Diese Art der Trickserei bei der Gestaltung wird *Dark Patterns* genannt – wörtlich: *Dunkle Muster*. Man könnte sie auch „betrügerisch", „unethisch" oder „Manipulation by Design" nennen.

Wenn wir gute Laune haben – und viel Zeit – können wir das Ganze auch als schräges Spiel betrachten – ein Dark-Pattern-Adventure: Schaffe ich, durch das Labyrinth zu kommen und alle Tracker abzulehnen? Was versuchen sie jetzt noch, um mich auszutricksen? Und wenn ich durchgekommen bin: Was war eigentlich nochmal der Artikel, den ich gerne lesen wollte? Ach, egal …

Cookie-Banner sind kein Spiel. Sie sind armselig und niederträchtig. Sie klauen mir meine Lebenszeit. Dieses Design will mich ermüden und zermürben. Es will, dass ich aufgebe und schließlich *OK* drücke.

Und jetzt einmal zum Mitschreiben: Nein, der Datenschutz ist nicht schuld! Nein, diese nervenden Abfragen sind vom Gesetz keineswegs so vorgeschrieben – vielmehr ist ein Großteil der Cookiebanner schlicht illegal. Die von Max Schrems[1] initiierte Datenschutzorganisation noyb.eu[2] hat Ende Mai 2021 mehr als 500 Beschwerden an Unternehmen verschickt, die auf ihrer Website rechtswidrige Cookie-Banner verwenden. Es könnten eine Menge mehr werden. Danke dafür! Ebenso Dank an die EU-Abgeordneten, die die Initiative trackingfreeads.eu[3] gegen personalisierte Werbung gestartet haben.

Dabei sind Cookie-Banner nur die sichtbare Materialisierung davon, wie wir im Internet ausgespäht werden.

Neben Cookies gibt es nämlich noch etliche andere Ausspähmethoden. Das Facebook-Pixel zum Beispiel, das unsichtbar auf vielen Medienseiten[4] eingebunden ist und unser Klickverhalten an Facebook verpetzt. Den Browser-Fingerabdruck, der Informationen über Betriebssystem, Browser, Plugins und installierte Schriften nutzt, um uns ganz ohne Cookies wiederzuerkennen.

Was mich wirklich wütend macht

Wissen Sie, was im Hintergrund passiert, wenn Sie eine Website „betreten"? Während die ersten Teile der Webseite laden, wird im Hintergrund Ihr persönliches Profil auf dem Werbemarkt feilgeboten. Es beginnt eine Auktion um Ihre Aufmerksamkeit. Sie sind die Ware. Das nennt sich *Real Time Bidding*, geschieht in Millisekunden. Verschiedene Gruppen von Online-Werbefirmen identifizieren, analysieren und kategorisieren Sie anhand Ihres Online-Profils, das wieder andere Werbefirmen verwalten. Nehmen wir mal an: Sie sind ein Mann, Mitte 40, mögen teure Uhren? Schwupps, zeigt Spiegel Online Ihnen BMW-Werbung. Oder die Studentin, die eben nach WG-Zimmern gesucht hat, versucht man direkt mit nur vermeintlich günstigen Kreditangeboten zu ködern.

Beim *Real Time Bidding* zockt ein ganzes Ökosystem von Werbefirmen darum, wer Ihnen seine Werbung zeigen darf. Ein gigantisches Netzwerk von Dienstleistern und Mit-Verdienern. Und die, die das Internet interessant machen, die Zeitungsverlage, Blogs, Inhalte-Lieferanten, bekommen am wenigsten vom Kuchen ab.

Was mich dann noch wirklich wütend macht, …

… sind die Leute, die rufen: Aber dafür sind doch die ganzen Inhalte gratis. Gratis? Hm – Ausforschung und Manipulation im Netz ist ein ziemlich hoher Preis für dieses „Gratis", finde ich. Dann wird behauptet: Die Medien, die die interessanten Inhalte produzieren, könnten ohne personalisierte Werbung gar nicht existieren. Das müssten wir doch einsehen und deshalb Tracking und personalisierte Anzeigen akzeptieren.

Das ist Quatsch. Medien haben auch früher schon Anzeigenplatz verkauft. Allerdings haben sie dabei bis in die 1990er Jahre den größten Teil der Einnahmen auch tatsächlich selber erhalten und konnten damit Journalisten, Fotografinnen, Zeichner, Rechercheurinnen etc. korrekt bezahlen. Seit den 2000er Jahren sind die Einnahmen der Medien im freien Fall. Denn inzwischen kommen 50–70 % (!) des Geldes, das die Anzeigenkunden ausgeben, gar nicht mehr bei den Verlagen an, sondern landen bei den Dienstleistern und Werbeplattformen, die sich dazwischen geschaltet haben.[5]

Und wo ist das Geld, das nicht mehr bei den Medien ankommt? Schauen Sie mal auf diese Grafik:[6]

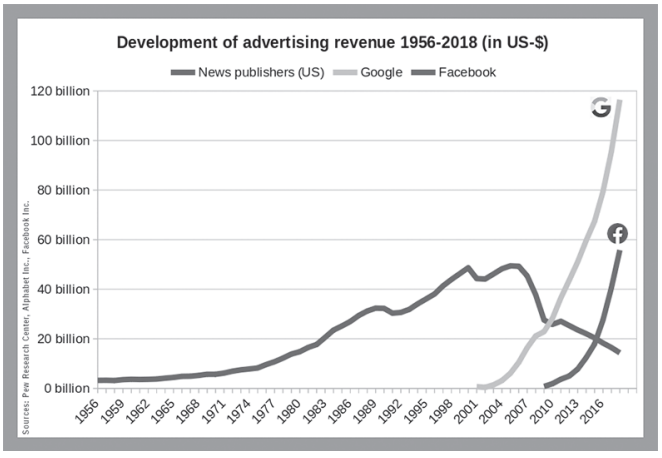


Diagramm: Development of advertising revenue 1956–2018

Inzwischen im Wesentlichen bei Google. Und bei Facebook. Ich fasse zusammen: Personalisierte Werbung bedeutet: Die Nutzer werden ausgehorcht – die Medien werden ausgehungert.[7]

Was mich wirklich wütend macht

Nun kommt Google als Ritter auf dem weißen Pferd daher und kündigt an: Chrome, der Google-eigene Browser, wird ab 2022 Third Party Cookies blockieren. Jubel im Netz und in den Medien: Google erlöst uns von den Cookie-Bannern!

Doch das Blockieren von Dritt-Partei-Cookies heißt mitnichten, dass das Tracking und die Ausforschung im Netz aufhören würde. Nein, Google will dafür einfach nur eine neue Technik einführen namens FloC – *Federated Learning of Cohorts*. FLoC bedeutet: Wir werden nach unserem Browsing-Verhalten der letzten Woche einer Gruppe von ein- bis fünftausend Individuen zugeschlagen, die ähnliche Websites besucht haben. Die Zugehörigkeit zu der jeweiligen Kohorte speichert Chrome auf unserem eigenen Rechner.

Wer jetzt denkt, dann zumindest in der Gruppe der tausend anderen untertauchen zu können, irrt sich. Zum Beispiel ist eine Person, die sich auf einer Website einloggt, natürlich nicht mehr anonym. Und ihre persönlichen Informationen können mit der aktuellen FloC-Kohorte verknüpft werden. Dasselbe gilt für alle, die einen Google- oder Facebook-Account haben und aus Bequemlichkeit ständig eingeloggt bleiben – auch die sind identifizierbar. Und schließlich können wir an unserem Browser-Fingerabdruck wiedererkannt werden. So sorgt FLoC dafür, dass wir in Zukunft noch genauer analysiert werden als bisher schon. Und der Chrome-Browser hat inzwischen einen Marktanteil von etwa 70 % weltweit.

FLoC ist keine datenschutzfreundliche Technik. Es beendet keineswegs unsere Verfolgung im Netz – eher im Gegenteil.[8] Aber wer könnte das auch ernsthaft von Google erwarten – einem Konzern, der 99 % seines Umsatzes mit Werbung macht. Eher glauben wir Piranhas, dass sie Veganer werden wollen.

Willkommener Nebeneffekt von FLoC und dem Blockieren von Third Party Cookies: Google bootet damit konkurrierende Werbeplattformen aus. Nicht, dass wir denen besonders nachweinen würden. Aber der Effekt wird sein, dass die Konzentration auf dem Werbemarkt noch weiter vorangetrieben wird. Google ist dort schon die Nummer eins, dann folgt Facebook und inzwischen auch Amazon. Und dann kommt lange nichts mehr. „Competition is for losers" – „Wettbewerb ist was für Verlierer."[9] Freier Markt? Ach was. Was man als Big Tech-Konzern will, ist ein Monopol.

Was mich wirklich wütend macht

Wie diese Konzerne mit uns umgehen. Wie sie Menschen nur noch als Rohstoff ansehen, den sie ausbeuten und deren persönliche Erfahrungen sie sich aneignen können. Die Verachtung für die Menschen, die Skrupellosigkeit und der Wille, sie über den Tisch zu ziehen. Die Verachtung fürs Steuerzahlen und für staatliche Infrastruktur. Und die Verachtung für geltendes Recht. Shoshana Zuboff hat ein Wort dafür gefunden: *Überwachungskapitalismus*.[10]

Es ist nicht nur eine einzelne Datenkrake – es ist ein ganzes krakiges Ökosystem. Dazu gehören die Versicherungen, die möglichst jedes Risiko für sich selber ausschließen wollen, die Scoring-Unternehmen, die uns geheime Noten geben, nach denen sich unsere Chancen im Leben richten, die Lobbyisten, die Think Tanks, die PR-Agenturen, die Anwaltskanzleien, die diese Enteignung möglich machen, und die Geheimdienste, die davon profitieren und selbst gern im Trüben fischen.

Und an wen geht denn nun dieser BigBrotherAward?

An die Cookie-Bäckereien? An die Internet-Werbewirtschaft? An die großen Plattform-Monopolisten? An die Nudging-Psychologen und die Dark-Pattern-Designer? Die Zeitdiebe und Nervenräuber? Die Profil-Dealer und Real-Time-Bidding-Casinobetreiber? Die Smarten, die Gewissenlosen und die Mitläufer bei den Medienhäusern? Die Karrieristen und die Blauäugigen unter den Digital-Politikern?[11]

Die Wahl fiel schwer.

Aber dann passierte etwas.

Was mich wirklich amüsiert hat

Denn Google hat sich quasi selbst nominiert.

Wir wissen nicht, ob es ein menschliches Versehen, die Heldentat eines Whistleblowers oder eine KI war, die digitales Wahrheitsserum genascht hatte …

Die Geschichte geht so: Zehn US-Bundesstaaten unter der Führung von Texas haben Ende 2020 Klage gegen Google eingereicht. Der Vorwurf: Google nutze seine Marktmacht, um Preise für Internetwerbung zu kontrollieren, ein Kartell zu bilden und Werbe-Auktionen zu manipulieren. Dafür nutze Google seine Mehrfachfunktion als Werbeplattformbetreiber, zugleich selber Werbeanbieter und seinen Zugriff auf Nutzerdaten hemmungslos aus. Der texanische General-Staatsanwalt Ken Paxton erklärte den Sachverhalt mit einem Bild aus dem Baseball: Google ist Werfer, Fänger und Schiedsrichter zugleich.[12]

Google schickte also Dokumente an das Gericht in Texas. Die waren zum Beweis seiner Unschuld gedacht. Die eingereichten Dokumente waren überaus relevant zu diesem Thema – allerdings so gar nicht in Googles Sinne. Denn die Dokumente wurden unredigiert eingereicht, also ohne die wirklich interessanten Stellen wirksam zu schwärzen.

Einige Stunden später bemerkte man bei Google den Irrtum und bat das Gericht, die Dokumente austauschen zu dürfen. Doch zu spät – ein paar flinke Gerichtsreporter des Jura-Portals MLex[13] hatten die unredigierte Fassung gelesen und flugs erkannt, was ihnen da für ein Schatz zugeflogen war:

Die Dokumente beschreiben, wie Google seit 2013 als Auktionsplattform seine Kenntnis von vorangegangenen Auktionen nutzt, um die voraussichtlich gerade ausreichenden Preise vorherzusagen. Damit konnten sie in ihrer zweiten Rolle als Werbevermittler aktuelle Anzeigenauktionen gewinnen, und zwar zu einem möglichst geringen Preis.[14] An der Börse heißt so etwas *Insiderhandel*. Vermutet wurde so etwas schon lange – nun steht es genau so in Googles eigenen Dokumenten.

Mit diesem Trick verschafft sich Google nicht nur einen Vorteil vor den anderen Werbevermittlern, sondern drückt auch den Preis, den Publisher für ihren Werbeplatz erhalten. Nutzer werden ausgeforscht – Medien ausgehungert.

Was mich wirklich wütend macht

Dieses Verfahren hat Google firmenintern *Project Bernanke* getauft – nach Ben Bernanke, dem ehemaligen Chef der US-Zentralbank. Dieser Codename bedeutet nichts anderes als „Googles Lizenz zum Gelddrucken". Welch eine Arroganz.

Damit aber nicht genug: 2018 hat Google mit Facebook, der Nummer 2 im Werbemarkt, eine geheime Abmachung geschlossen – interner Codename *Jedi Blue*. Darin sichert Google seinem Konkurrenten Facebook zu, dass sie 10 % der Anzeigenauktionen, an denen sie auf Googles Plattform teilnehmen, gewinnen. Wie soll das gehen in einem Markt mit angeblich freiem Wettbewerb?

Nun: Google liefert Facebook dafür Informationen über Netznutzer:innen, anhand derer Facebook 60 % der Desktopnutzer und 80 % der Mobilnutzer eindeutig identifizieren kann. Damit weiß Facebook, bei wem es sich lohnt, in Anzeigen zu investieren. Facebook sagt im Gegenzug zu, dass sie eine bestimmte Summe für Anzeigen investieren und dass sie ein geplantes Verfahren namens *Header Bidding*, das anderen Werbenetzwerken neben Google bessere Chancen gegeben hätte, nicht weiter verfolgen. Wenn das keine Wettbewerbsmanipulation ist, was dann?

Aber: Erwischt!

Rena Tangens – Foto: Matthias Hornung CC BY-SA 4.0

Was mir Mut macht!

Die Klagen und Bußgeldverfahren gegen Big Tech wegen Datenschutz- und Wettbewerbsverstößen häufen sich, sowohl von einzelnen Ländern (aktuell in Frankreich) wie auch von der EU und in den USA. Jawoll – geltendes Recht durchsetzen![15]

Kalifornien – ja, der US-Bundesstaat, in dem auch Silicon Valley liegt – hat ein Datenschutzgesetz beschlossen. Vorbild war das europäische Datenschutzrecht – doch das kalifornische Gesetz ist tatsächlich strenger![16]

Die *New York Times* hat 2018 (nach Inkrafttreten der DSGVO) beschlossen, für ihre internationale Ausgabe auf Tracker und personalisierte Werbung zu verzichten und schaltet Anzeigen nun wieder kontextabhängig. Neben dem Plus an Datenschutz ist diese Entscheidung auch ein finanzieller Erfolg: Denn weil die Tracking-Dienstleister nun außen vor sind, bleibt mehr vom Werbegeldkuchen für die Zeitung übrig.[17]

Die britische Tageszeitung *The Guardian* hat 2019 nach schwierigen Jahren zum ersten Mal mit einem satten Plus abgeschlossen – ganz ohne Paywall, mit Spenden der Leserinnen und Leser.[18]

Die EU bereitet zwei wichtige Verordnungen vor, die in das Geschäft der Internet-Riesen eingreifen: Den *Digital Services Act* (DSA) und den *Digital Markets Act* (DMA). Die Lobbyisten und die Anwaltskanzleien von Big Tech sind schon am Rotieren.[19]

Was uns extra Schwung geben sollte: In den USA entwickelt sich tatsächlich eine überparteiliche Bewegung, die die Macht der großen Digitalkonzerne beschneiden will. Wir freuen uns auf Lina Khan[20], die von Joe Biden für die Federal Trade Commission (FTC, die Verbraucher- und Wettbewerbsbehörde) nominiert wurde – eine kompetente Kritikerin von Big Tech.[21]

Und: Google erhält den BigBrotherAward 2021 für jüngst offenbar gewordene massive Manipulation des Internet-Werbemarktes, Aushungern von Kreativen und Medien sowie Enteignung unserer digitalen Persönlichkeiten.

Vielleicht ist das alles schon mal der Anfang von etwas, was Google wirklich wütend macht.

Herzlichen Glückwunsch, Google.

Referenzen

Zuboff S (2018) Das Zeitalter des Überwachungskapitalismus. Frankfurt / New York

Zuboff S (2019) The Age of Surveillance Capitalism. The Fight for a Human Future at the new Frontier of Power

Morozov E (2013) To Save Everything, Click Here: The Folly of Technological Solutionism

Thema: Dark Patterns

Forbrukerradet – Norwegian Consumer Council: Deceived by Design. How tech companies use dark patterns to discourage us from exercising our rights to privacy. 27.06.2018, https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf

Dark Patterns als Online-Spiel: Terms & Conditions Apply, https://termsandconditions.game/

Sehr schönes Video zu Cookie-Bannern von Stevie Martin, https://twitter.com/5tevieM/status/1375116382770171906

Thema: Googles FLoC – Federated Learning of Cohorts

EFF: Google's FLoC is a terrible idea, March 3, 2021, by Bennett Cyphers, https://www.eff.org/deeplinks/2021/03/googles-floc-terrible-idea

Herausfinden, ob FLoC schon auf dem eigenen Rechner aktiviert ist: https://amifloced.org/

Thema: Tracker, Facebook Pixel, Super Cookies, Browser Fingerprint

Tracking-ID aus Favicons: Datensammler erfinden immer neue Supercookies, https://t3n.de/news/tracking-id-favicons-supercookie-1355514/

Bin ich im Netz wiederzuerkennen?
Hier den Browser-Fingerabdruck testen:
https://amiunique.org/
https://coveryourtracks.eff.org/

Thema: Personalisierte Anzeigen abschaffen

IAB Paper: What would an Internet without targeted ads look like? https://iabeurope.eu/wp-content/uploads/2021/04/IAB-Europe_What-Would-an-Internet-Without-Targeted-Ads-Look-Like_April-2021.pdf

Umfrage zu personalisierten Anzeigen: Globalwitness.org: Do people really want personalised ads online? https://www.globalwitness.org/en/blog/do-people-really-want-personalised-ads-online/

Die wahren Kosten von personalisierten Anzeigen: The costs of tracking ads – Tracking ads harm journalism, https://trackingfreeads.eu/the-costs-of-tracking-ads/

Thema: Wettbewerbsmanipulation – Googles „Project Bernanke" und „Jedi Blue"

MLex, 7.42021: Google acknowledges it foresaw possibility of probe of ‚Jedi Blue' advertising deal with Facebook. By Michael Acton, Mike Swift, https://mlexmarketinsight.com/news-hub/editors-picks/area-of-expertise/antitrust/google-acknowledges-it-foresaw-possibility-of-probe-of-jedi-blue-advertising-deal-with-facebook

MLex, 9.4.2021: Google's description of ‚Jedi Blue' clarifies states' US antitrust complaint. By Mike Swift, Michael Acton, https://mlexmarketinsight.com/news-hub/editors-picks/area-of-expertise/antitrust/googles-description-of-jedi-blue-clarifies-states-us-antitrust-complaint

Wall Street Journal, 11.4.2021: Google's Secret 'Project Bernanke' Revealed in Texas Antitrust Case. Program used past bid data to boost tech company's win rate in advertising auctions, according to court filing. Jeff Horwitz and Keach Hagey, https://www.wsj.com/amp/articles/googles-secret-project-bernanke-revealed-in-texas-antitrust-case-11618097760

welt.de, 24.04.2021: Das „Projekt Bernanke" entlarvt Googles wahre Macht. Von Benedikt Fuest, https://www.welt.de/wirtschaft/article230613523/Projekt-Bernanke-und-FloC-So-trickst-Google-im-Werbemarkt.html

Anmerkungen

1 *Max Schrems hat schon 2015 hier bei den BigBrotherAwards auf der Bühne gestanden und hat als Gastlaudator unseren Innenministern die Leviten gelesen, weil sie – während sie eifrig das Gegenteil behaupteten – versuchten, das europäische Datenschutzrecht zu schwächen. Hier seine Laudatio: https://bigbrotherawards.de/2015/politik-thomas-de-maiziere-hans-peter-friedrich*

2 *noyb.eu – none of your business https://noyb.eu/de*

3 *https://trackingfreeads.eu/the-costs-of-tracking-ads/*

4 *Wie zum Beispiel Zeit Online – unser BigBrotherAwards-Preisträger des Jahres 2019. Hier die Laudatio: https://bigbrotherawards.de/2019/verbraucherschutz-zeit-online*

5 *https://trackingfreeads.eu: https://trackingfreeads.eu/the-costs-of-tracking-ads/*

6 *https://trackingfreeads.eu/wp-content/uploads/2021/05/Chart-ad-revenue.png*

7 *Wall Street Journal, 29.5.2019: Behavioral Ad Targeting Not Paying Off for Publishers, Study Suggests. https://www.wsj.com/articles/behavioral-ad-targeting-not-paying-off-for-publishers-study-suggests-11559167195*

8 *Die EFF fasst es so zusammen: „FLoC ist das Gegenteil einer datenschutzfreundlichen Technik. Während Ihnen heute noch Tracker durchs Web folgen, in den digitalen Schatten herumschleichen, um zu erraten, was für eine Art Person Sie wohl sind, werden die sich in Googles Zukunft zurücklehnen, entspannen und den Browser auf Ihrem Rechner die Arbeit für sich machen lassen." Übersetzung Rena Tangens, Quelle: https://www.eff.org/deeplinks/2019/08/dont-play-googles-privacy-sandbox-1*

9 *Zitat von Peter Thiel, Gründer von Paypal und Palantir, Investor bei Facebook*

10 *Shoshana Zuboff: The Age of Surveillance Capitalism, https://shoshanazuboff.com/book/about/ – Artikel von Shoshana Zuboff in der FAZ: https://www.faz.net/aktuell/feuilleton/debatten/the-digital-debate/shoshana-zuboff-secrets-of-surveillance-capitalism-14103616.html*

11 *Oder doch die Werbefachleute, Marktforscher, Unternehmensberater, Versicherungsvertreter und Telefondesinfizierer – die, wie wir aus Douglas Adams' „Per Anhalter durch die Galaxis" wissen – vom Planeten Golgafrincham evakuiert wurden und auf der Erde gelandet sind?*

12 *Syracuse Law Review, 24.12.2020: https://lawreview.syr.edu/google-as-the-pitcher-batter-and-umpire-the-latest-in-the-war-against-big-tech/*

13 *MLex, 7.4.2021: Google acknowledges it foresaw possibility of probe of ‚Jedi Blue' advertising deal with Facebook by Michael Acton, Mike Swift https://mlexmarketinsight.com/news-hub/editors-picks/area-of-expertise/antitrust/google-acknowledges-it-foresaw-possibility-of-probe-of-jedi-blue-advertising-deal-with-facebook*

14 *Businessinsider, 21.4.2021: The 5 most revelatory findings about Texas' antitrust fight against Google, including the secret ‚Project Bernanke' and its ‚Jedi Blue' deal with Facebook https://www.businessinsider.com/5-highlights-from-the-texas-ag-antitrust-case-versus-google-2021-4*

15 *Bundeskartellamt: Verfahren gegen Google, 25.5.2021: https://www.bundeskartellamt.de/SharedDocs/Meldung/DE/Pressemitteilungen/2021/25_05_2021_Google_19a.html Tagesschau.de, 7.6.2021, Millionenstrafe für Google in Frankreich. https://www.wsj.com/articles/behavioral-ad-targeting-not-paying-off-for-publishers-study-suggests-11559167195 Tagesschau.de, 9.12.2020: US-Staaten verklagen Facebook. https://www.tagesschau.de/wirtschaft/facebook-us-bundesstaaten-103.html*

16 *Ionos, 15.1.2021: California Consumer Privacy Act: https://www.ionos.de/digitalguide/websites/online-recht/california-consumer-privacy-act-ccpa/*

17 *Digiday, 19.1.2019, After GDPR, The New York Times cut off ad exchanges in Europe — and kept growing ad revenue https://digiday.com/media/gumgumtest-new-york-times-gdpr-cut-off-ad-exchanges-europe-ad-revenue/*

18 *Meedia.de, 2.5.2019: The Guardian vermeldet erstmalig seit 1998 schwarze Zahlen – und hat nicht mal eine Paywall. https://meedia.de/2019/05/02/the-guardian-vermeldet-erstmalig-seit-1998-schwarze-zahlen-und-hat-nicht-mal-eine-paywall/*

19 *Lobbycontrol, 15.12.2020: DSA/DMA – wie Big Tech neue Regeln für digitale Plattformen verhindern will. https://www.lobbycontrol.de/2020/12/dsa-dma-wie-big-tech-neue-regeln-fuer-digitale-plattformen-verhindern-will/*

20 *Lina Khan: http://www.linamkhan.com/work*

21 *Sueddeutsche.de, 15.3.2021: Juristisches Wunderkind. https://www.sueddeutsche.de/wirtschaft/kartellrecht-amazon-monopol-usa-1.5235952 Manager Magazin, 11.3.2021: Die Jägerin der digitalen Monopole bekommt Macht in Washington. https://www.manager-magazin.de/lifestyle/lina-khan-die-jaegerin-der-silicon-valley-monopole-bekommt-macht-in-washington-a-0fa02dad-b447-4af3-89e0-1c45475ab2f7*

FIfF-Konferenz 2021 – München, *12.-14. November 2021*

Foto: Reinald Kirchner, CC BY-SA 4.0

Selbstbestimmung in digitalen Räumen

Denn man sieht nur die im Lichte, die im Dunkeln sieht man nicht.

Die zunehmenden undurchsichtigen (Vor-) Entscheidungen, Klassifikationen, Scoring- oder Filterfunktionen digitaler Helfer wirken auf uns als Einzelpersonen: Wird mein Antrag auf Umschulung abgelehnt, weil der Score für eine erfolgreiche Vermittlung zu schlecht ist? Aber sie wirken auch auf uns als Gesellschaft: Wer verarbeitet womöglich diskriminierend welche Informationen? Wenn technische Systeme – von Konzernen für ihre Zwecke optimiert – autonom entscheiden, sollten wir als Gesellschaft verhandeln, was wir für wünschenswert und konstruktiv halten (ausführlichere Motivation siehe auch *FIfF-Kommunikation* 1/2021 und *2021.fiffkon.de*). Schließlich verbringen wir mit unseren elektronischen Geräten mehr Zeit als mit unseren Freunden oder der Familie. Ohne sie ginge gar nichts mehr, weil sie wichtige Arbeitsmittel und bequeme, allzeit bereite Helfer im Alltag sind.

Mittlerweile haben wir das Programm für die Münchner Tagung weitgehend geplant. Wir werden sie digital und – abhängig von der aktuellen Pandemie-Lage – auch vor Ort durchführen.

Hauptprogramm

Fest eingeplant sind eine Reihe von interessanten Vorträgen, die uns einen Überblick zu den verschiedenen Facetten einer fehlenden digitalen Selbstbestimmung geben. Wir planen dabei jeweils auch Zeit für Diskussionen ein, um Handlungsmöglichkeiten auf individueller und auf gesellschaftlicher Ebene zu diskutieren.

- Digitale Risikokompetenz: Wer steuert unser Verhalten?
  Gerd Gigerenzer vom Harding-Zentrum für Risiko-kompetenz, Universität Potsdam

- Kontrollierte Selbstbestimmung. Wie Überwachung im Gesundheitswesen unter die Haut geht.
  Silja Samerski vom Fachbereich Soziales und Gesundheit, Hochschule Emden

- Strafrecht, algorithmische Prädiktionen und das zero-trust-Paradigma: Braucht Zukunft Vertrauen durch Konflikt?
  Christoph Burchard vom Fachbereich Rechtswissenschaft der Goethe-Universität Frankfurt am Main

- Digitale Gesellschaft zwischen Herrschaft und sozialer Innovation
  Philip Staab, Lehrbereich Soziologie der Zukunft der Arbeit der Humboldt-Universität Berlin

- Welche Versprechungen für die Verbesserung des (sozialen) Lebens kann Automated Decision-Making halten und welche nicht? Potenzial und Grenzen automatisierter Fehlerreduktion in sozialen Daten.

Frauke Kreuter, Fakultät für Sozialwissenschaften an der Universität Mannheim & Institut für Statistik an der Ludwigs-Maximilians-Universität München

- Voreingenommenheit im Gehirn und im Algorithmus
  Abigail Morrison vom Institute for Advanced Simulation, Forschungszentrum Jülich

- Die soziale Konstruktion von Algorithmen
  Heiner Heiland, Fachbereich Soziologie der TU Darmstadt

- Wer hat das Sagen über digitale Infrastrukturen? Historische und ethnografische Beobachtungen
  Monika Domman, Historisches Seminar der Universität Zürich

Abstracts zu den Vorträgen werden wir im September auf der Konferenz-Homepage veröffentlichen (zu finden über *2021.fiff.kon.de*).

Ergänzen werden wir das Hauptprogramm durch eine Podiumsdiskussion, in der wir vor allem aus praktischer, nach Möglichkeit auch aktivistischer Sicht diskutieren wollen, wie wir unseren bedrohten Freiraum der Selbstbestimmung im Digitalen retten oder wieder herstellen können. Durch ein konkret zu diskutierendes Anwendungsgebiet wollen wir die Erkenntnisse aus den Vorträgen und den Diskussionen in individuelle und gesellschaftliche Handlungsfelder übersetzen.

Schultrack

Parallel zu seinem Hauptprogramm bietet das FIfF bei seiner diesjährigen Jahreskonferenz einen Schultrack an: Schüler, Eltern und Lehrer können sich zum Internet, alternativen Programmen, Chancen und Risiken informieren. Vorträge und Workshops sollen SchülerInnen und ErzieherInnen anregen, sich mit Technik kritisch auseinander zu setzen.

Zusammen mit Chaos Computer Club München (*muc.ccc.de*), digitalcourage (*digitalcourage.de*), Free Software Foundation Europe (*FSFE.org*) und dem Berufsverband der Datenschutzbeauftragten in Deutschland (*bvdnet.de*) möchten wir mit Euch in Vorträgen, Workshops und auf einem Podium diskutieren. Der Schultrack findet parallel zum Hauptprogramm statt und spricht Kinder und Jugendliche ab 6 Jahren an.

Workshops

Zudem bieten wir auf dieser Tagung Raum für ergänzende Workshops, die genauen Rahmenbedingungen werden wir veröffentlichen, wenn die Durchführung der Tagung geklärt ist (wenn die Veranstaltung vor Ort stattfinden kann).

Die FIfF-Konferenz ist öffentlich. Der Eintritt ist frei. Für Verpflegung wird am Wochenende gegen einen Unkostenbeitrag gesorgt.

Einladung zur Mitgliederversammlung 2021

des Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF e. V.)

Wir laden fristgerecht und satzungsgemäß zur ordentlichen Mitgliederversammlung 2021 ein.
Sie findet am Sonntag, den 14. November 2021, von 12:00 bis 15:00 Uhr statt.
Der Ort (München/online) wird unter *2021.fiffkon.de* rechtzeitig bekannt gegeben.

Vorläufige Tagesordnung

1. Begrüßung, Feststellung der Beschlussfähigkeit und Festlegung der Protokollführung
2. Beschlussfassung über die Tagesordnung, Geschäftsordnung und Wahlordnung
3. Bericht des Vorstands einschließlich Kassenbericht
4. Bericht der Kassenprüfer
5. Diskussion der Berichte
6. Entlastung des Vorstands
7. Neuwahl des Vorstands
8. Neuwahl der Kassenprüfer
9. Diskussion über Ziele und Arbeit des FIfF, aktuelle Themen, Verabschiedung von Stellungnahmen, Berichte aus den Regionalgruppen
10. Anträge an die Mitgliederversammlung
    Anträge müssen schriftlich bis drei Wochen vor der Mitgliederversammlung bei der FIfF-Geschäftsstelle eingegangen sein
11. Verschiedenes

gez. Stefan Hügel
für den Vorstand und die Geschäftsstelle des FIfF

Marit Hansen

Dr. Waus Chaos Computer Film – Alles ist eins. Außer der 0.

Eine Filmempfehlung[1]

Vor 20 Jahren ist Wau Holland gestorben. Er war Mitgründer des Chaos Computer Clubs und Wegbegleiter des Datenschutzes. Jetzt sind Filmdokumente mit ihm und über ihn in die Programmkinos gekommen.

Für ihre Zeitreise in die Vergangenheit von Hacking, Netzpolitik und Datenethik holen die Regisseur:innen Klaus Maeck und Tanja Schwerdorf weit aus: Albert Einstein macht den Anfang, recht schnell springt der Film zum Kalten Krieg und dann in die 1970er Jahre mit teils schriller Subkultur und ganz verschiedenen Communities von Punk, Science-Fiction-Büchern, LSD und Antiatomkraftbewegung. Der Erzähler Peter Glaser führt die Zuschauer:innen durch die Geschichte und bringt alles in einen Zusammenhang: wie nämlich all diese Subkulturen Einfluss hatten auf die Menschen und die Ideen, die sich zur deutschen Hackerbewegung rechnen lassen. Diese Aufgabe erfüllt Peter Glaser tadellos, er macht keine Umschweife, verbindet die – von gelegentlichen Anspielungen auf filmische Referenzen oder Memes abgesehen – nüchterne Darstellung mit sympathischem österreichischen Tonfall, ist beschreibender Beobachter. Und er ist gleichzeitig viel mehr, denn er war dabei: Auch wenn sich Peter Glaser zurücknimmt, ist er doch selbst ein Teil der Geschichte.

Der Film begleitet Wau Holland ab Ende der 1970er Jahre bis zu seinem Tod. Seine Lebensgeschichte wird verbunden mit dem Chaos Computer Club (CCC), der deutschen Netzpolitik und der rasanten Entwicklung der Digitaltechnik. Den Bogen zur heutigen Zeit spannt der Film mit Darstellungen zu den Enthüllungen von Edward Snowden und Chelsea Manning, zu Wikileaks und Julian Assange und zu heutigen biometrischen Überwachungsmöglichkeiten.

Der Journalist Wau Holland – eigentlich Herwart Holland-Moritz – gehörte zu den Gründern des CCC. Die bis heute gültige Forderung des CCC „Öffentliche Daten nützen, private Daten schützen" verdeutlicht die Wichtigkeit von Informationsfreiheit auf der einen Seite und Datenschutz auf der anderen Seite.

Ein Film über Hacking, aber kein Hacker-Film: Die Dokumentation will natürlich kein Hollywood-Streifen à la *Wargames*, *Sneakers*, *Das Netz* oder *Staatsfeind Nr. 1* sein. Die Geschichte um Wau Holland ist nicht ausgedacht und für ein Millionenpublikum konstruiert, sondern sie nimmt vorhandenes Material, um ein Bild von Wau und dem Chaos Computer Club zusammenzusetzen. Die Regisseur:innen mussten dabei auswählen, was gezeigt und was weggelassen wird. Gar nicht so einfach, denn die Berichte zum eher kuriosen BTX-Hack oder zum doch eher riskanten Nasa-Hack dürfen nicht fehlen, doch ist das beschriebene Hacking etwas viel Größeres: „Was ist denn das, einen Rechner aufzumachen, dagegen, eine Gesellschaft aufzumachen."[2]

Genau dieses Weiterdenken, teils visionär, teils (durchaus auch absichtlich) verschroben – eben prägend für die Hacker-Subkultur, die sich allmählich den Weg zum Mainstream bahnte – war ein Anliegen für Wau Holland. Er brachte die Beispiele, half auf die Sprünge, um Konsequenzen zu erkennen, und machte seine Punkte auf eine ruhige, oft auch dozierende Art, was ihm den Spitznamen „Dr. Wau" beschert hatte. Die damaligen Erkenntnisse, die man in dem Filmmaterial (noch einmal) hört, sind (leider) weiterhin aktuell: Komplexe Systeme lassen sich schwer – oder gar nicht – beherrschen. Aus Daten mit lächerlich geringem Informationsgehalt kann man ein detailliertes Bild über eine Person konstruieren. Dieses Bild muss aber gar nicht stimmen. Mit Auslassung von Informationen kann man manipulieren.

Wie im Film herausgearbeitet, war in der deutschen Geschichte das mangelhafte Informieren der staatlichen Stellen im Krisenfall Tschernobyl bedeutsam für das Engagement von Zivilgesell-

schaft: Die Bevölkerung hätte sich mehr verlässliche Informationen über den Nuklearunfall im Kernkraftwerk am 26. April 1986 mit einer Ausbreitung radioaktiver Stoffe auch in Deutschland und die Nachbarländer gewünscht. Schon damals wollten sich viele Bürger:innen dies nicht mehr gefallen lassen. Noch war das Recht auf Informationszugang in Deutschland unbekannt, sodass behördliche Informationen nur in gesetzlich geregelten Ausnahmefällen öffentlich angefragt werden konnten.[3] Der Chaos Computer Club konnte nachweisen, dass die Bundesregierung fehlerhaft oder sogar manipulativ über die Strahlenbelastung informiert hatte, und setzte sich für das Gegenmodell ein: nämlich korrekte und vollständige behördliche Daten zur Verfügung zu stellen.

Gleichzeitig sollten und sollen vertrauliche Daten vertraulich bleiben. Dass es (immer mal wieder) einen Schulterschluss zwischen Chaos Computer Club und den Datenschutzbeauftragten gab, ist keineswegs eine Selbstverständlichkeit. Zwar hatte Wau Holland schon nach dem BTX-Hack auf der DAFTA (Datenschutzfachtagung) im November 1984 auftreten dürfen und im Interview zum Thema „Datenschützer" kommentiert, sie hätten einen falschen Namen, da es nicht darum ginge, Daten zu schützen, sondern Menschen vor dem Missbrauch von Daten.[4] Doch nur wenige Chefs der Datenschutzbehörden hatten keine Berührungsängste, wenn es um die Frage ging, ob man CCC-Aktivisten auch zu Veranstaltungen als Vortragende oder Mitwirkende einladen solle.

Im Film werden viele öffentliche Auftritte von Wau Holland gezeigt – davon steht Videomaterial zur Verfügung. Was ebenfalls verfügbar ist, sind zahlreiche Archivierungen von Postings, z. B. in der Usenet-Newsgroup de.org.ccc.[5] Wau Holland war bewusst, dass man mit der Zusammenstellung selektiver korrekter Informationen – z. B. aus den „Flames", in die er über die Zeit verwickelt war – ein Zerrbild mit gehässigen Kommentaren erzeugen könne. Er erahnte schon die Effekte von Big Data und künstlicher Intelligenz, die wir heute immer mehr erleben. Aber auch mit zahlreichen Einspielern und Zeitdokumenten bleibt offen, wie der Privatmensch Wau Holland war. Rastlos, selbstbestimmt bis hin zum Raubbau an der eigenen Gesundheit – so weit nähert sich der Film an. Ein kreativer Macher, der sich – mal charmant, mal nonchalant und auch mal provokativ – über den bestimmungsgemäßen Gebrauch von Dingen hinwegsetzt.[6] Mit anarchischer Hippie-und-Technik-Attitüde – was kaum mal in Kombination vorkommt. Das wirklich ganz Persönliche und Private? Selbst bei seiner Bestattung sprach der Vater von Wau Holland von wichtigen politischen Maximen wie der, dass von deutschem Boden nie wieder Krieg ausgehen dürfe.[7] Dieser Punkt der Privatperson Wau Holland muss offen bleiben; falls die Filmemacher:innen mehr wissen, respektieren sie seine Privatsphäre und sparen dies aus.

Wau Holland war nicht nur Visionär sondern auch Vorreiter im Bereich Medienkompetenz. Das betrifft auch Frauen und Mädchen im Technikbereich – ein Thema, das im Film weitgehend ausgespart ist. Es kommen sogar erstaunlich wenige Frauen vor. In einem Video aus dem Jahr 1999 verdeutlicht Wau Holland, was in der Gesellschaft zu dem Zeitpunkt bisher noch nicht erreicht war, gerade im Schul- und Bildungsbereich[8]: Während in England die Kinder seit 1984 bereits in der ersten Klasse Computer-Unterricht hätten, käme in Deutschland Informatik im Schul- und Bildungsbereich viel zu wenig vor. In England seien daher bei den unter 18-jährigen Internet-Nutzenden etwa die Hälfte Mädchen. Wäre damit nur die Bedienung von Smartphones und Computern als Konsument:in gemeint, könnte man dies heutzutage als *erreicht* abhaken. Wer Wau aber zuhörte, wusste, dass es ihm nicht nur um die Benutzung der Technik ging, sondern um das Verständnis für das gesamte technische System und die gesellschaftlichen Implikationen. Heute sind Forderungen nach Informatik-Unterricht nicht mehr revolutionär, aber immer noch nicht flächendeckend in der Praxis umgesetzt.

Ein Großteil der (*Boomer*-)Leserschaft wird selbst die 1980er und 1990er Jahre erlebt und sich auch dann schon für technische, freiheitsrechtliche oder gesellschaftliche Themen interessiert haben. All diese Personen werden durch den Film in die damalige Zeit ein Stück weit zurückgeworfen und sich wieder erinnern, wie es damals war. „Du brauchst ein Modem." – So ging es damals nicht nur beim Erzähler Peter Glaser los. Auch das Science-Fiction-Buch „Der Schockwellenreiter" von John Brunner, aus dem Wau Holland in einer Filmszene im Publikum stehend vorliest, wurde damals mehr oder weniger zerlesen von Hand zu Hand gereicht.

Eine der zahlreichen Filmkritiken schreibt, dass die filmische Geschichtsstunde bis 2001 bemerkenswert gut funktionieren würde, aber mit dem Tod des eigentlichen Protagonisten Holland deutlich an Fahrt verlieren würde.[9] Die Autorin beurteilt dies anders: Gerade der letzte Teil des Films zeigt einerseits die Weitsicht des Visionärs und Fast-schon-Propheten Wau Hollands, andererseits aber die Notwendigkeit, seine Ideen und Gedanken nicht nur abgeklärt oder staunend im Rückblick zur Kenntnis zu nehmen, sondern etwas für die faire Ausgestaltung der digitalen Welt zu tun. Einige Aktionen des Chaos Computer Clubs werden herausgehoben. „You have to take action" ruft uns dann auch Edward Snowden zu. Chelsea Manning spricht von den „ethical obligations that we as developers have"[10]. Und der Film endet mit der Nachricht „We can hack back"[11].

Marit Hansen

Marit Hansen, Landesbeauftragte für Datenschutz Schleswig-Holstein. Hatte die Ehre, für die Kino-Dokumentation „Alles ist eins. Außer der 0." als Filmpatin ernannt zu werden. Und sie hatte das Glück, Wau Holland gekannt und erlebt zu haben. Sie bedankt sich bei allen Zeitzeug:innen, die sie haben teilhaben lassen an eigenen Erlebnissen mit Wau, sodass sie sich selbst wieder erinnerte: an die Stimmung anlässlich der Volkszählung, an ihre Anfangsjahre vom Informatikstudium und dem Beruf im Datenschutz, an „Datenreisen"-Treffs mit Fachsimpeleien zu Akustikkopplern, Modems und Mailboxen – und schließlich an ihre eigenen Begegnungen mit Wau in Kiel, Hamburg und Thüringen.

Aber unsere Geschichte endet natürlich auch dann nicht. Denn der Film war schon lange abgedreht und nur wegen der Pandemie erst jetzt in die Kinos gekommen. Und ohnehin kann man bei solchen Dokumentationen nicht vollständig auf die aktuellen Herausforderungen eingehen. Denn die aktuelle Entwicklung ist besorgniserregend, wie die Nachrichten über die Ausnutzung von Sicherheitslücken mit der Spionagesoftware „Pegasus" auch in Europa, über die Kontrolle privater Chat-Nachrichten oder über politische Beschlüsse zur Staatstrojanern oder Vorratsdatenspeicherung zeigen. Es ist wichtig, in der Geschichte zurückzuschauen, um einiges besser zu verstehen und daraus zu lernen. Doch es ist kein bequemer Film, mit dem man sich berieseln lassen kann: In der heutigen Realität von Informationsfreiheit und Datenschutz sind die Probleme nach wie vor sehr relevant und längst nicht gelöst. Alles ist eben eins. Ach ja: Außer der 0.

Zum Weiterlesen und -hören:

Informationen über den Film „Alles ist eins. Außer der 0.": https://allesisteins.film/

NPP233 mit Klaus Maeck „Wau Holland war die Seele des Chaos Computer Clubs", Podcast von Markus Beckedahl, 24.07.2021, https://netzpolitik.org/2021/npp233-mit-klaus-maeck-wau-holland-war-die-seele-des-chaos-computer-clubs/

Archiv aller Ausgaben der „Datenschleuder" (seit Ausgabe Nr. 1 von 1984): https://ds.ccc.de/download.html

Daniel Kulla: Der Phrasenprüfer. Szenen aus dem Leben von Wau Holland. Grüner Zweig, 2003.

John Brunner: Der Schockwellenreiter, 1975.

Anmerkungen

1 *Siehe auch Pressemitteilung der Autorin: Wau Holland, Wegbegleiter des Datenschutzes, in der Kino-Dokumentation „Alles ist eins. Außer der 0.", 30.07.2021, https://www.datenschutzzentrum.de/artikel/1379-.html*

2 *Zitat von Wau Holland in: Nika Bertram, Radio Wauland – Wie Hacker die digitale Welt verbessern wollten, Hörspiel des Westdeutschen Rundfunks, 2011, https://www1.wdr.de/radio/wdr3/programm/sendungen/wdr3-hoerspiel/wau-holland-daten-sicherheit-hacker-100.html*

3 *Im Bund und in der Mehrzahl der Bundesländer gelten mittlerweile Transparenz- oder Informationsfreiheitsgesetze, aber die Bereitstellung von Informationen der öffentlichen Hand ist immer noch keine Selbstverständlichkeit.*

4 *ZDF heute journal vom 15.11.1094: Wau Holland auf der DAFTA, https://www.youtube.com/watch?v=Sk8kKUTFXBE&t=258s.*

5 *Beiträge mit oder über Wau Holland archiviert unter https://groups.google.com/g/de.org.ccc/search?q=wau%20holland*

6 *Claus Schönleber: 15 Jahre: You never dies, say we, https://www.schoenleber.org/wau/.*

7 *Andy Müller-Maguhn: „Schon Wau Holland, der Gründer des CCC, hatte einen sehr politischen Ansatz. Er ist noch vor seinem Vater gestorben, und an seinem Grab hat sein Vater von der unschönen deutschen Vergangenheit gesprochen. Nie wieder soll von deutschem Boden Krieg ausgehen, hat er gesagt – das war der Kommentar eines Vaters beim Begräbnis seines Sohnes. Das hat für mich eine Menge erklärt, warum Wau so sehr auf andere eingewirkt und sich um sie gekümmert hat, warum er so friedfertig mit ihnen umgegangen ist, warum er Ideen verbreitet hat, statt sie zu beschränken, und warum er nicht aggressiv aufgetreten ist und so viel Wert auf Zusammenarbeit gelegt hat." In: Assange, Appelbaum, Müller-Maguhn, Zimmermann: Cypherpunks: Unsere Freiheit und die Zukunft des Internets, 2013.*

8 *Tim Pritlove: Wau Holland auf dem Chaos Communication Camp 1999, https://www.youtube.com/watch?v=oGjuESv8wRs&t=114s,*

9 *Max Muth: Kino-Dokumentation über den Chaos Computer Club: Computerliebe, 27.07.2021, https://www.sueddeutsche.de/kultur/alles-ist-eins-ausser-der-0-chaos-computer-club-dokumentarfim-1.5365383*

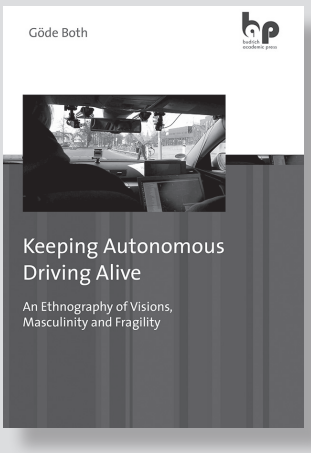
10 *re:publica 2018 – Opening Fireside Chat with Chelsea Manning, 03.05.2018, https://www.youtube.com/watch?v=lYFP7-zb6J4&t=705s.*

11 *Alexander Hacke: We Can Hack Back (feat. Ed Snowden), https://www.youtube.com/watch?v=F1kESXZq3R0.*

Britta Schinzel

Göde Both: Keeping Autonomous Driving Alive: An Ethnography of Visions, Masculinity and Fragility

Dies ist eine höchst interessante ethnografische Studie über ein Forschungs- und Entwicklungsprojekt zum autonomen Fahren. Schon der Titel läßt ahnen, dass es hier sich nicht um eine begeisterte Fortschritts-Erzählung handelt. Vielmehr entfalten sich in der begleitenden Beobachtung der Entwickelnden eines Projekts zum Autonomen Fahren, AutoNOMOS, die ungeheuren Schwierigkeiten, denen sie sich angesichts der Komplexität der Aufgabe ausgesetzt sehen, und die nicht nur für das universitäre Einzel-Projekt einen Erfolg fragwürdig erscheinen lassen. Dabei ist schon die Bedeutung autonomen Fahrens weder selbstverständlich, noch ist der Begriff ex ante auch nur einigermaßen klar definiert. Würden Autos, so wie Bahnen auf Schienen, in einen einigermaßen begrenzten und abgeriegelten Halbtunnel gesetzt, oder erhielten sie eine eigene, abgeschottete Fahrspur, so wäre das wohl durchführbar. Aber allein das Überholen wäre



Göde Both
Keeping Autonomous Driving Alive: An Ethnography of Visions, Masculinity and Fragility, Budrich Academic Press, 2020, Opladen, Berlin, Toronto
150 Seiten
ISBN 978-3-96665-009-0
pdf unter
https://library.oapen.org/handle/20.500.12657/48367

auch so ein schwer zu bewältigendes Problem. Zu fehleranfällig sind die Sensortechnik, die Bilderkennung unter Licht-, Wetter- und sonstigen Bedingungen, zu störanfällig das Machine Learning aus einer Datenerhebung unter sich dynamisch veränderlichen Kontexten, das laufend neu zu erlernende Umweltbedingungen vorfindet. Wohl kaum wird es je möglich sein, autonome Autos durch unsere alten Städte oder auf Landstraßen in Wald und Feld fahren zu lassen.

Aber die Diskussion solcher Fragen ist eigentlich nicht Thema dieses Buches, sondern die Begleitung der Forschenden im Projekt, das natürlich bestimmten Visionen folgt, Erwartungen und Versprechungen erfüllen will. Für diese gilt es, einen Kontext zu fabrizieren, in dem ein technologisches Projekt insoweit realisierbar wird, dass es die gewünschte Aufmerksamkeit erregt. Die Erwartungen sind also generativ, indem sie Struktur und Legitimierung erzeugen, Interesse wecken und Investitionen anlocken.

Der Autor entfaltet im Anfangskapitel eine profunde theoretische Basis der Methoden in den Bereichen der humanistischen Sozialwissenschaften, der Science Technology Studies und der Gender Studies. Das Forschungsdesign für eine noch wachsende Technologie ist notwendigerweise chaotisch, uneindeutig, instabil und unsicher. Daher kann auch das Ergebnis der ethnographische Studie nicht eindeutig sein. Für solche Projekte ist die Verwendung der Aktor-Netzwerk-Theorie geeignet. Zudem erlaubt sie, in einer Feldstudie nicht nur mit sozio-kulturellen, symbolischen Fragen, sondern auch mit der Materialität solch technologischer Projekte umzugehen. So kann er sein Forschungsdesign passgenau auf das von ihm untersuchte Feld, das Projekt AutoNOMOS an der Freien Universität Berlin richten. Ein besonderer Aspekt dieses Projektes war die Frage nach der Maskulinität der Vision autonomen Fahrens, während gleichzeitig zu erwarten ist, dass die Entwicklung neuer Transporttechnologien, die nicht an den hegemonialen Besitz privater Autos gebunden sind, die Ausübung von Männlichkeit destabilisieren würde.

Narrative und Erzählungen steuern die Erwartungen, Versprechungen und Visionen dieses Projekts. Im zweiten Kapitel wird der Weg von den visionären Erzählungen unter den Bedingungen der verteilten Arbeit an Computern hin zu autonomen Versuchsfahrten ausschließlich männlicher Informatiker, zumeist Robotiker, dargestellt. Sie arbeiten vorwiegend am Computer, haben aber ein Labor mit prototypischen Fahrzeugen zur Verfügung, das sie mit Physikern teilen. Diese Fahrzeuge, MiGs genannt, haben zwei Rollen, einerseits als Forschungsinstrumente und andererseits als Demonstratoren u. a. für die Medien und die Projektträger.

Die Versuchsfahrten bilden die eigentliche *Reale-Welt*-Herausforderung für das Projekt. Hier erst zeigt sich, was alles zusammen bedacht, kontrolliert und beobachtet werden muss, was das Mosaik visionärer Erzählungen kontinuierlich auf den Boden der tentativen Machbarkeiten reduziert. Alle Projekte zum autonomen Fahren haben eine gemeinsame Gegnerschaft, die von fast allen europäischen Ländern ratifizierte U. N. *Vienna Convention on Road Traffic*, die verlangt, dass jedes Fahrzeug einen menschlichen Fahrer haben muss. Wenn also autonomes Fahren als unüberwacht angenommen werden soll, dann ist es auf öffentlichen Straßen illegal. Versuchsfahrten müssen daher einerseits als Ausnahmeversuche lizensiert sein und bedürfen zweitens eines Sicherheitskonzepts, das garantiert, dass die autonomen Fahrzeuge im Verkehr keine Gefahr für manuell gesteuerte Fahrzeuge darstellen. Diese Anforderungen führten im untersuchten Projekt dazu, dass kaum eine Institution bereit war, solche Versuchsfahrten zu gestatten, bis sich endlich ein privater Träger fand.

Im dritten Kapitel werden die *Real-world*-Situationen auf einer gestatteten Teststrecke dargestellt. Das Testfahrzeug wird zwar über einen intern angebrachten Laptop über ein *car-to-computer-interface* gesteuert und überwacht, doch nach wie vor muss eine zweite Person vor dem Lenker sitzen. Der Laptop prozessiert Sensordaten und konstruiert ein Weltmodell, in dem er sich selbst als Fahrzeug lokalisiert, um durch den Verkehr zu navigieren. Die Repräsentation der Teststrecke repräsentiert nur eine beschränkte Anzahl von GPS-Punkten, die durch den Laptop verknüpft werden, ein Prozess, der Trajektorien-Generation genannt wird. Verschiedene potenzielle Wege werden generiert und einige selektiert, die bestimmten Anforderungen genügen. Ergebnis ist ein Plan, welcher sodann für die Teststrecke verfolgt wird. Die Aufgaben sind also das Abbilden der Umgebung, die Lokalisierung des Fahrzeugs darin, die Wegeplanung und die Kontrolle des Fahrzeugs. Andere Verkehrsteilnehmer werden als Hindernisse auf den Trajektorien repräsentiert. Für sie werden drei Arten von Ressourcen genutzt, um den Verkehr zu verstehen: A-priori-Repräsentationen, Vermessungen und szenariobasierte Regeln. Kommt ein solches Hindernis vor das Fahrzeug, wird der Plan gestoppt und das Fahrzeug abgebremst. Für den Fahrer, der inaktiv im Auto sitzen muss, ist es eine sehr anstrengende Herausforderung, die Instrumente des Wagens nicht zu bedienen, auch wenn Fußgänger oder andere Fahrzeuge in die Nähe kommen. Both identifiziert diese androzentrische Subjektposition als den „einsamen entkörperten Fahrer". Die Vorstellung kombiniert ein physikalistisches Verständnis des Verkehrs mit einer mechanistischen Anwendung eines legalen Verkehrscodes. Um die Komplexität der Situation zu reduzieren, personifizieren und anthropomorphisieren die experimentierenden Forscher das Fahrzeug als männlichen Charakter und verwischen so die Unterscheidung zwischen Auto und Fahrer.

Im vierten Kapitel befasst sich Both mit den meist männlichen Entwicklern und stellt überrascht fest, dass sie keineswegs Autofreaks sind, die sich mit schnellen Wettfahrten identifizieren, manche kommen mit dem Fahrrad zur Arbeit. Nach der Verbindung zwischen dem automotiven Projekt und Männlichkeit befragt, stellen sie diese in Frage: Die „Gehirnarbeit" der Informatik sei geschlechtsneutral im Gegensatz zur Arbeit mit physischen technologischen Artefakten. Umso interessanter ist das Herausarbeiten der Frage, ob, und wenn ja, wo die Sicherung des automatischen Fahrens als maskulines Projekt stattfindet. Jedenfalls wird es als ein Wettstreit um Vollautomatisierung verstanden. Auch das Zelebrieren des Fahrens in sportlicher Manier beim Herumbasteln an Software und der Hand am Auto widerspricht dem Ideal eines komfortablen, effizienten und sicheren Transports, der zentral in der Vorstellung des Projekts ist. Am Ende ergibt sich symbolisch wohl die hierarchische Höherstufung, wenn sich simultan zwei Formen technischer Expertise verbinden: die mechanischen Kompetenzen bei der Modifikation von Fahrzeugen mit den analytischen Kompetenzen mathematischer Programmierung in der Robotik und noch einmal in Verbindung mit KI. Beide sind traditionell mit Maskulinität ver-

knüpft. Dafür sprach die Identifikation eines der Projektteilnehmer wie eines Knight Riders aus der Science Fiction-Literatur, wo Robotik, KI und selbst-lernende Autos in einem ernsthaften Spiel fusionieren, all dies durchaus als männlich angesehene Aktivitäten.

Da der Erfolg des Projekts gegenüber den Geldgebern dokumentiert werden muss, sind die Video-Demonstrationen ein wichtiger Teil des Projekts. Im fünften Kapitel wird die subtile Arbeit der heroischen Erzählung zwischen Fake und Wirklichkeit beschrieben, wobei sich der Demonstrator in der *Double-Bind*-Situation befindet, einerseits ein erfolgreiches Ziel in Aussicht stellen und gleichzeitig die Erwartungen realistisch beschränken zu müssen. Am Ende, im 6. Kapitel beschrieben, müssen die Entwickelnden ihre Arbeit verteidigen, aber auch vor sich selbst rechtfertigen, manche indem sie den technischen Erfolg preisen, andere indem sie das Projekt nicht als ein realistisches, als ein irreales, ansehen.

Die Arbeit schließt mit einem Kapitel über Care als zwar unsichtbarer, aber zentral notwendiger (symbolisch feministischer) Aspekt des Projekts in einer dynamisch veränderlichen Einbettung, im Kontext der Sorge um eine vom autonomen Fahrzeug nicht kontrollierbare Umgebung. Die verkörperte Kommunikation zwischen der Straße und ihren anderen Nutzenden entgleitet der androzentrischen Imagination, die in der Konfiguration des MiG projektiert ist. Im MiG transportiert zu werden fühlt sich an wie das Fahren in einer Bahn mit unsichtbaren Schienen, und nicht wie Autofahren. Dies steht im Gegensatz zur Maskulinität (Robotiker) und den visionären Narrativen (Wettstreit um die Bewältigung der Materie), die das Projekt leiten.

Ein sehr ausführlicher Literaturteil beschließt das Buch.

Das Lesen dieser Arbeit ist sehr zu empfehlen, zeigt sie doch die Komplexität all der Verknüpfungen und Verknotungen von symbolischen, technischen, realweltlichen, politischen und juristischen Aspekten, Förderungs-politischen und Arbeitskontexten der Mammut-Aufgabe in einer Nussschale eines solchen eingebetteten System-Projekts und demonstriert in unnachahmlicher Weise, mit welchem (und nur so) aufwändigen theoretischen und methodologischen Apparat sich der begleitenden Analyse des Projekts genähert werden kann.

Wissenschaft & Frieden 3/2021: Frieden lernen, aber wie? – Aktuelle Fragen der Friedenspädagogik

Immer drängender stellt sich in Zeiten der globalen Multikrise die Frage danach, wie Frieden gefunden werden kann: Frieden mit uns selbst, mit unseren Mitmenschen, mit dem belebten Planeten, mit der Welt? Friedensbildung kommt dabei eine zentrale Rolle bei der Ausbildung der menschlichen Friedfähigkeit und Friedfertigkeit zu. Die Ausprägung friedlichen Handelns, Denkens und Fühlens, aber auch die Kritik und Überwindung gewaltförmiger Strukturen und Verhältnisse stehen dabei im Zentrum. W&F erkundet aktuelle Fragen und Herausforderungen im Feld der Friedensbildung, thematisiert theoretische und strukturelle Lücken und problematisiert die Unterfinanzierung.

Dabei wird klar: Friedensbildung nimmt aktuell wichtige Impulse aus anderen (Fach-)Diskursen zu Pädagogik jenseits kolonialer Kontinuitäten oder epistemischer Gewalt auf, erlebt einen enormen Bedeutungszuwachs und versucht sich an einer Vielzahl kreativer, anti-hierarchischer Methoden – von Theater über ungewöhnliche Lernsettings bis hin zur Frage nach dem Lernen in transpersonaler Verbundenheit. Dabei helfen auch Erfahrungen anderer Kontexte und Gemeinschaften aus aller Welt. In dieser globalen Verbundenheit des Wissens und der radikalen Pädagogiken hofft Friedensbildung ihren Beitrag zur Veränderung der Multikrise(n) zu leisten.

Außerhalb des Schwerpunktes finden sich zwei Beiträge zu aktuellen Konflikten: den Protesten in Kolumbien und ihren strukturellen Ursachen widmet sich Stefan Peters, dem Abzug aus dem *Desaster* in Afghanistan schenkt Matin Baraki kritische Aufmerksamkeit. Zudem stellen wir eine Methodenstudie zur Messung des *Spillover* zwischen Rüstungs- und ziviler Industrie vor.

W&F 3/21 | August | 68 Seiten | 12€ (print) / 9€ (epub) | *wissenschaft-und-frieden.de*

Stefan Hügel

Nils Melzer: Der Fall Julian Assange. Geschichte einer Verfolgung

Seit über zehn Jahren erleben wir die politische Verfolgung von Julian Assange, der mit seiner Organisation Wikileaks das Ziel hat, Kriegsverbrechen und andere kriminelle Handlungen von Staaten und Wirtschaftsorganisationen publik zu machen und damit Transparenz in staatliches und wirtschaftliches Handeln zu bringen. Besonders bekannt wurde das Video *Collateral Murder*[1], das den Beschuss und die Tötung von Journalisten und Zivilisten (darunter auch Kinder) durch eine US-amerikanische Hubschrauberbesatzung und deren höhnische Kommentare dazu zeigt. Fast genauso lang werden er und seine Unterstützer:innen, genannt seien hier Chelsea Manning[2] und Reality Winner[3], von Behörden verfolgt und drakonisch bestraft – dabei spielen vor allem US-amerikanische, britische und schwedische Polizei- und Sicherheitbehörden eine wesentliche Rolle. Jahrelang musste Assange in der Londoner Botschaft von Ecuador Zuflucht suchen, bis er den dortigen Machthabern nach einem Regierungswechsel lästig geworden war und den britischen Behörden ausgeliefert wurde. Eine Auslieferung in die USA, wo ihm die absurde Strafe von 175 Jahren Freiheitsentzug[4] droht, wurde durch ein britisches Gericht zunächst abgelehnt – dennoch ist er dort immer noch inhaftiert, in einem Hochsicherheitsgefängnis. Auch die deutsche Bundesregierung hat es bisher versäumt, deutlich für Transparenz und Menschenrechte Stellung zu beziehen und sich für die Freilassung von Assange einzusetzen.

Nils Melzer, Sonderberichterstatter der Vereinten Nationen für Folter und Autor des hier besprochenen Bandes bezeichnet den Fall als einen der größten Justizskandale aller Zeiten:

> *„Wir müssen aufhören zu glauben, dass es bei Julian Assange wirklich um eine Strafuntersuchung wegen Sexualdelikten, Spionage und Hacking geht. Was Wikileaks getan hat, bedroht die politischen und wirtschaftlichen Eliten weltweit gleichermaßen. Der Fall Assange zeigt, dass es den Regierungen heute nicht mehr um legitime Vertraulichkeit geht, sondern um die Unterdrückung der Wahrheit zum Schutz von unkontrollierter Macht, Korruption und Straflosigkeit“,*

so der Umschlagstext des Buches. Solche deutlichen Worte sind bemerkenswert von einem Mann, der qua Amtes auch politische Rücksichten nehmen muss.

Der Band zeichnet den Fall Assange nach, aus Sicht des Autors, der einen ersten Appell von Assanges Anwälten beiseite schob – handelte es sich nicht um einen Sexualstraftäter, Vergewaltiger? Also ein Verbrechen, das gerade in heutiger Zeit, sicherlich zu Recht, als besonders gravierend eingestuft wird – deswegen aber auch tabuisiert ist. Wir erinnern uns noch an die Debatten, ob Assange auf einem Chaos Communication Congress angehört werden sollte[5]. Nähere Beschäftigung mit dem Fall führte bei Melzer zur Überzeugung, dass es sich hier tatsächlich um gravierende Menschenrechtsverletzungen handelte. Eine nähere Untersuchung der Vorwürfe der Vergewaltigung ließen Fragen aufkommen: Wurde der Vorwurf den davon betroffenen Frauen untergeschoben? Polizeiliche Vernehmungsprotokolle gefälscht? In einer liberalen Demokratie wie Schweden? Die Erkenntnisse von Nils Melzer wären unter anderen Umständen kaum zu glauben, aber Melzer ist eben nicht irgendwer. Nochmal: Es ist der von den Vereinten Nationen benannte Sonderberichterstatter für Folter. Er schließt auch ausdrücklich nicht aus, dass sich Assange der genannten Taten schuldig gemacht hat, weist ausdrücklich darauf hin, dass er nur die Ungereimtheiten beschreibt, die er bei der Befassung mit dem Fall festgestellt hat.

Nils Melzer (2021):
Der Fall Julian Assange.
Geschichte einer Verfolgung.
Piper-Verlag, München, 2021
336 Seiten
Preis: € 22,00 (Hardcover)
EAN 978-3-492-07076-8

Auf die Vorwürfe und die daraus resultierende Verfolgung folgt das jahrelange Asyl in der ecuadorianischen Botschaft und die teilweise unwürdigen Bedingungen, die Ausweisung aus der Botschaft und Verhaftung durch die britische Polizei, die Inhaftierung im Hochsicherheitsgefängnis *Belmarsh*, in dem sonst Terroristen einsitzen, der Prozess, der – letztlich überraschend – mit der Abweisung der Auslieferung an die USA endete, aber nicht mit Assanges Freilassung.

Auch die Position der deutschen Bundesregierung ist fragwürdig. Während sie zu Alexei Nawalny engagiert Stellung bezog, hielt sie sich zu Assange merklich zurück. Auch der Vorsitzende der Grünen, Robert Habeck, kam schwer ins Stottern, als er zu seiner Position zu Assange befragt wurde.[6] Wovor haben diese Leute Angst?

Vieles, was in diesem Buch zu lesen ist, möchte man kaum glauben. Sitzt man hier einer Verschwörungserzählung auf? Nein, wohl nicht, die Person des Autors und die öffentlich bekannte Entwicklung sprechen gegen eine solche Folgerung.

Mit Transparenz wird die Hoffnung verbunden, dass sie Demokratie möglich mache und Menschenrechtsverletzungen verhindere. Das Verfahren und die Ereignisse um Julian Assange fanden und finden aber vor den Augen der Weltöffentlichkeit statt – ohne Konsequenzen für den Verlauf des Verfahrens oder die Verantwortlichen.

Das Buch empfehle ich jedem, der sich mit grundlegenden Fragen von Transparenz, Menschenrechten und staatlicher Machtpolitik auseinandersetzen möchte. Die Authentizität der einzelnen Details ist naturgemäß schwer zu beurteilen – hier kann

man sich nur auf die Medienberichte der letzten Jahre[7] und die Vertrauenswürdigkeit des Autors[8,9] verlassen. In Summe ist das Material, das hier zusammengetragen wurde, erschreckend und weckt Zweifel an der Funktionsfähigkeit unserer demokratischen Rechtsstaaten.

Anmerkungen

1 *Video auf Wikileaks, https://collateralmurder.wikileaks.org*
2 *Wikipedia, Stichwort Chelsea Manning, https://de.wikipedia.org/wiki/Chelsea_Manning*
3 *Wikipedia, Stichwort Reality Winner, https://de.wikipedia.org/wiki/Reality_Winner*
4 *Der Spiegel, https://www.spiegel.de/ausland/wikileaks-prozess-julian-assange-drohen-in-den-usa-175-jahre-haft-a-5fbe0716-1a67-4264-a399-6b572b42eff1*
5 *Süddeutsche Zeitung, https://www.sueddeutsche.de/digital/konferenz-des-chaos-computer-clubs-assange-kritiker-stoeren-video-uebertragung-1.1853271*
6 *Interview Tilo Jung mit Robert Habeck, https://www.youtube.com/watch?v=qtMDubgHcYw*
7 *Stellvertetend für viele The Guardian, https://www.theguardian.com/media/2019/apr/11/how-ecuador-lost-patience-with-houseguest-julian-assange*
8 *Wikipedia, Stichwort Nils Melzer, https://de.wikipedia.org/wiki/Nils_Melzer*
9 *Seite von Nils Melzer bei den Vereinten Nationen, https://www.ohchr.org/en/issues/torture/srtorture/pages/nilsmelzer.aspx*

Dagmar Boedicker

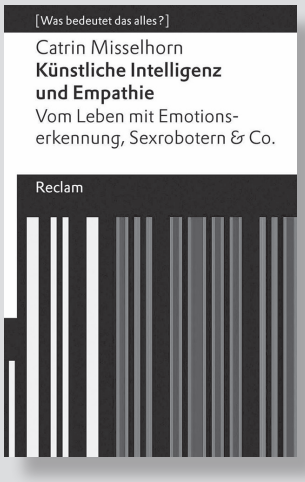
Catrin Misselhorn: Künstliche Intelligenz und Empathie

Es ist nicht das erste Buch der Philosophin Catrin Misselhorn zum Verhältnis zwischen angewandter Philosophie und Technik. Mit Grundfragen der Maschinenethik *lieferte sie eine solide, verständlich und prägnant geschriebene Einführung mit Blick auf die gesellschaftlichen Aspekte. Auch der neue Titel ist wieder sehr klar und verständlich. Beide Bücher sind bei Reclam erschienen.*

Nach einer kurzen Darstellung von starker und schwacher KI und maschinellem Lernen nimmt Misselhorn den Begriff der emotionalen künstlichen Intelligenz auf, die aus einer Notwendigkeit entwickelt worden sei, Emotionen als Antriebe menschlichen Verhaltens zu verstehen. Mir gefällt, wie sie Begriffe einführt und dabei im Zusammenhang verschiedener Disziplinen definiert, beispielsweise der Hirnforschung oder der Philosophie. Den Überblick über die Emotionstheorien fasst sie in einer Tabelle zusammen, unterscheidet basale und komplexe Emotionen und erklärt, wie und warum KI sich mit den basalen Emotionen befasst.

Es geht zunächst um das Erkennen von Bewegungen des Gesichts, der Mimik, und ihre Kodierung in Bewegungseinheiten *(FACS, Facial Action Coding System)* nach Paul Ekman[1]. Eigenschaften des Sprechens ordnet die stimmbasierte Emotionserkennung in ein Koordinatensystem ein, in dem sich Emotionen als Vektoren darstellen lassen. In der Analyse einer Gesprächssituation können die Parameter in Bezug auf Lautstärke, Tonhöhe, Sprechgeschwindigkeit, Anzahl von Pausen oder Ins-Wort-Fallen ausdifferenziert werden. Daraus lassen sich Zuschreibungen von Persönlichkeitsmerkmalen, gern von Arbeitsuchenden, oder Strategien für die Manipulation ableiten.

> *„Einige Firmen haben Apps entwickelt, um an die entsprechenden Daten zu kommen. […] Die […] App bringt Menschen dazu, die stimmbasierte Emotionserkennung spielerisch auszuprobieren. Dabei generier[t] sie Daten, um das System zu trainieren. Das Programm soll für über 25 Sprachen funktionieren, […]. In der Coronakrise arbeitete Vocalis Health daran, anhand von Stimmanalyse Hinweise auf eine Infektion mit Covid-19 zu gewinnen." (Seite 31)*



Catrin Misselhorn
Künstliche Intelligenz und Empathie – Vom Leben mit Emotionserkennung, Sexrobotern & Co.
Reclam Verlag, Ditzingen, 2021
181 Seiten
Preis € 12,00 (Hardcover)
ISBN: 978-3-15-011344-8

Unser Gesicht oder unsere Stimme haben wir nicht so recht unter Kontrolle und wissen das auch. Und den Sprachgebrauch? Damit befasst sich die Sentimentanalyse, mit bekannten Folgen beispielsweise als Manipulation von positiven oder negativen Einstellungen in den *sozialen* Netzen oder als die willkürliche, Empathie-freie Suche nach *Verdächtigen*. Im Abschnitt zu den technischen und ethischen Fragen findet sich eine Tabelle mit der systematischen Aufstellung von Einsatzbereichen für emotionale KI, Zwecke und Methoden (Seite 45 ff.).

Da sich Emotionen meist auch körperlich bemerkbar machen, lassen sich Bio-Sensoren wie die beliebten Fitness-Tracker nutzen. Solche Systeme sind besonders ambivalent: Einerseits können sie Menschen helfen, ihre physische und psychische Gesundheit im Blick zu behalten und positiv zu beeinflussen, anderseits bieten sie der Unterhaltungs-Industrie fantastische Möglichkeiten, die

Erlebnisse der Nutzerïnnen mit Hilfe höchst sensibler Daten Gewinn-maximierend anzufeuern. In den falschen Hände sind die Informationen der Emotionserkennung ein Unglück.

Wenn ein Computer mit Menschen zu tun bekommt, wie in der Pflege, der Bildung, bei Spielen, soll *artifizielle Empathie* helfen, ihn zu einem akzeptierten sozialen Gegenüber zu machen. Software-Modelle sollen verschiedene Komponenten der Empathie berechen- und implementierbar machen, entweder theoriebasiert, datengetrieben oder in einer Kombination beider Methoden (Seite 68 ff.). Die Autorin stellt zwei praktische Bespiele vor, den Pflegeroboter *NICA* und das DARPA-geförderte[2] System *Ellie* für die psychologische Diagnose, beide wissenschaftlich begleitet und dokumentiert. Es zeigte sich, dass Menschen „leicht bereit [sind], künstliche Systeme als empathisches Gegenüber wahrzunehmen." (Seite 88) Da bei Menschen das Schmerzempfinden ein wichtiger Aspekt ist, wenn sie Empathie und daraus soziales und moralisches Verhalten erlernen, geht es im nächsten Abschnitt um die Biorobotik, die sich an der Nachbildung des Nervensystems versucht.

> *„Ethisch hätte es jedenfalls weitreichende Konsequenzen, Lebewesen herzustellen, die über Schmerzbewusstsein verfügen. Denn ihnen käme aufgrund ihrer Natur ein intrinsischer (also von den Interessen der Menschen unabhängiger) moralischer Status zu, der zumindest mit demjenigen von Tieren vergleichbar wäre." (Seite 107)*

Empathie mit Robotern?

Menschen nehmen Systeme als empathisches Gegenüber wahr, haben sie auch Mitgefühl mit ihnen? Misselhorn schildert in einem kleinen Ausflug in die Science Fiction, vor allem ins Kino, welche Gefühle geweckt wurden. Meist ging es um menschenähnliche KIs, mal war Empathie im Spiel, mal fehlte sie schmerzhaft. Obwohl sich bei Menschen Empathie mit KI feststellen lässt, schreiben sie ihr deswegen doch keine Emotionen zu. Wegen der Verbindung zwischen Empathie und moralischen Urteilen fragt Misselhorn nun nach moralischen Verpflichtungen gegenüber Robotern. Ein Schema zeigt, wie auf dem Weg von Schmerz-Empfindung über Empathie und die negative affektive Bewertung ihres Bezugsgegenstands ein allgemeines moralisches Urteil entsteht. Das Schema lässt sich kaum auf Roboter übertragen, weil wir – anders als bei Tieren – nicht glauben, dass sie Schmerz empfinden. (Seite 116) Unsere perzeptuelle Empathie lässt sich aber nicht selektiv ausschalten und das Ausschalten sollte deshalb nicht zur Gewohnheit werden:

> *„Unter der Voraussetzung, dass es moralisch geboten ist, die Quellen des eigenen moralischen Urteilens nicht zu beeinträchtigen, folgt daraus ein indirektes Argument dafür, dass wir Roboter nicht misshandeln sollten. Denn dies würde die Fähigkeit, Empathie mit anderen Menschen zu empfinden, beeinträchtigen, die eine Quelle moralischer Urteile ist." (Seite 119)*

So würde die moralische Entwicklung von Kindern gestört, „wenn sie sich – aktiv oder passiv – an die Misshandlung[3] humanoider Roboter gewöhnen." (Seite 123 f.)

Freundschaft, Liebe und Sex mit Robotern

Nach der kurzen Vorstellung *sozialer Roboter* als „subjektsimulierende" Maschinen und dem Verweis auf Sherry Turkle, die sich schon in den 1990ern damit beschäftigt hat, hebt die Autorin hervor, dass wir uns dringend mit den ethischen und sozialen Fragen der sozialen Robotik beschäftigen sollten, weil sie schon bald Teil unseres Alltags sein könne. So seien Sexroboter auf dem Vormarsch. Misselhorn beschreibt die Gestaltung der Maschinen und stellt sie in den Gender- und kulturspezifischen Zusammenhang. Sie zitiert Quellen, die

> *„[…] zeigen, dass es bereits jetzt eine Subkultur von Männern gibt, die eine Art von Beziehung mit ihren Sexpuppen leben, und diese – ganz im Sinn von Sherry Turkles Begriff relationaler Artefakte – als etwas ansehen, das zwischen Lebewesen und Ding angesiedelt ist. […] Zudem verstärkten Sexroboter die ohnehin bereits jetzt offensichtliche gesellschaftliche Tendenz, Frauen als Objekte zu betrachten, über die Männer frei verfügen können. […] Zudem leisteten echte zwischenmenschliche Beziehungen einen wichtigen Beitrag für den gesellschaftlichen Zusammenhalt, dessen Zerstörung durch Sexroboter zur Zunahme ökonomischer und sozialer Ängste, psychischer Erkrankungen und Isolation führe." (Seite 137 f.)*

Die These der Autorin ist, dass „das Subjekt in einer solchen Beziehung letzten Endes selbst zum Ding wird." (Seite 153) Durch einen solchen, der Zwischenmenschlichkeit ausweichenden Technikeinsatz (Solipsismus) entstehen Probleme für die Gesellschaft, Beziehungen können sich zuspitzen und gesellschaftliche Tendenzen verschärfen. Es fehlt die genuin soziale Beziehung, die nur zwischen menschlichen Subjekten entstehen kann. Misselhorn bezieht sich auf den Sozialphilosophen Axel Honneth, der

> *„unterscheidet zwischen drei Formen der Anerkennung, die für die Herausbildung einer gelingenden praktischen Identität ausschlaggebend sind: Liebe, Respekt und soziale Wertschätzung."*

In einer Liebesbeziehung erleben sich beide Partner

> *„als Wesen mit Bedürfnissen, zu deren Erfüllung sie auf die empathische und sorgende Anteilnahme des jeweils anderen angewiesen sind. Nur in der wechselseitigen Anerkennung ihrer Bedürfnis- und Affektnatur können die Individuen zu einer positiven Einstellung gegenüber den eigenen Bedürfnissen gelangen sowie eine grundlegende Form des Selbstvertrauens und des Gefühls für ihren eigenen Wert entwickeln." (Seite 154 f.)*

Das ist unmöglich, wenn das KI-Gegenüber weder Bedürfnisse hat noch Gefühle und nicht mit Empathie auf Gefühle reagieren kann. Die Autorin bezeichnet die Liebe zu einem Roboter als „verzerrte Form einer sozialen Praxis" und grundsätzlich ungeeignet für wechselseitige affektive Annerkennung.

Im Geschäftsmodell des Überwachungskapitalismus gehen Bedürfnisse und Gefühle verloren, Menschen sind Objekt des

Messens, Bewertens, Beobachtens und der Manipulation. Emotionale KI kann das besonders gut und „macht das subjektive emotionale Innenleben, das Personen ausmacht, selbst zum Gegenstand der Vermessung und Manipulation." Die Autorin kritisiert die unzureichende Rechtsgrundlage für die Vermessung und Manipulation und fehlende Möglichkeiten der Gegenwehr gegen deren Eingriffe in „fundamentale Lebensbereiche und Chancen […]"

Ihren Ausblick auf das Projekt empathische KI bezeichnet Misselhorn als verhalten, sie geht davon aus, dass sich die Kooperation zwischen Mensch und Maschine auf Anerkennungstheoretisch aussichtsreicheren Wegen erreichen lässt. Sie sieht sinnvolle Anwendungen von Robotern im therapeutischen Bereich und mahnt zu gewissenhafter Begleitung und dem Einsatz nur in sorgfältig ausgesuchten Situationen. Für Freundschaft und Liebe sollten wir uns besser weiterhin an Menschen halten.

Die Philosophin kombiniert in ihrer Betrachtung wissenschaftliche Nüchternheit und Schlüssigkeit mit konkreten Beispielen. Rundum zu empfehlen!

Anmerkungen

1 *der mit CIA und Homeland Security der USA zusammenarbeitete*

2 *Defense Advanced Research Projects Agency des US-Verteidigungsministeriums*

3 *Der Begriff Misshandlung ist hier definiert als: „jede Art von absichtlicher Handlung, die – wenn sie an einem Menschen ausgeführt wird – erhebliche körperliche oder geistige Schmerzen verursachen würde, wie Schlagen, Treten oder Beleidigen." (Seite 113) Eine moralische Bewertung ist mit dem Begriff nicht verbunden.*

Dagmar Boedicker

Jean Peters: Wenn die Hoffnung stirbt, geht's trotzdem weiter

Das ist ein politisches Buch – keine Frage. Was sollte der Tortungs-Künstler vom Kollektiv Peng! auch anderes schreiben als „Geschichten aus dem subversiven Widerstand"? Und wie könnten diese Geschichten langweilig sein, wenn sie von solchen Aktionen handeln? Es ist ein anregendes Buch in lähmenden Corona-Zeiten.

Peng! ist eine deutsche Aktionskunst-Gruppe, die der Buchautor Jean Peters gegründet hat, *The Yes Men* aus den USA sehr ähnlich. Peters schreibt konsequent aus der Wir-Sicht, er spielt nicht sich in den Vordergrund sondern erzählt von der vielen Arbeit vieler Menschen, die hinter den Aktionen stehen und sie erst möglich machen. Es hat meine FIfF-Seele ungemein gefreut, über so viel Kreativität und Witz zu lesen, das macht Spaß. Dabei geht es nicht nur um die satirische Seite; *Peng!* zeichnet sich durch eine wohlüberlegte Betrachtung der Ziele, Rahmenbedingungen und möglichen Folgen aus: Es gibt ein solides theoretisches Fundament, zusammengefasst im deutschsprachigen *Critical Campaigning Manifesto* auf Seite 228f (eher kein Lesevergnügen für Menschen, die mit dem *Gendering* hadern). Da steht, was wir bei Kampagnen und, wie ich finde, auch sonst für achtsame politische Arbeit bedenken sollten. Ab Seite 52 geht es ausführlich um die kritische Reflexion der eigenen Position[1] und die Inhalte und Motivation von Aktionskunst. Peters geht immer wieder auf einzelne Punkte des Manifests ein.

Alles also vorbildliche Arbeit da, wo sich Kunst und Politik verbinden, auch wenn die eine oder andere Aktion nicht lief wie geplant, die mit den biometrischen Passfotos beispielsweise *(Fluchthelfer.in* 2015). Es ist schon so: Aufklärung über die Mechanismen von Macht muss heute zu oft die Satire leisten, nachdem *soziale Netze* entgegengesetzt wirken und es den medialen Türstehern immer weniger um Inhalte zu gehen scheint:

> *„Politische Debatten gleichen mehr und mehr Inszenierungen, eigentliche politische Entscheidungsprozesse werden immer weniger inhaltlich diskutiert. Es geht immer mehr um Personalien, um Überschriften, um Gesten. […] Und während das Vertrauen in die Politik weiter erodiert, kommen uns langsam die Fakten abhanden.*

Jean Peters
Wenn die Hoffnung stirbt, geht's trotzdem weiter
S. Fischer Verlag, Frankfurt, 2021
251 Seiten
Preis € 21,00 (Hardcover)
ISBN: 978-3-10-397087-6

> *Von Kellyanne Conway, der Beraterin des ehemaligen Präsidenten Donald Trump, als ‚Alternative Facts' eingeführt […]" (Seite 69)*

Wer wollte dem widersprechen? Das x-te Buch, das solche Kulturkritik oder politikwissenschaftlichen Erkenntnisse endlos akademisch ausbreitet, hätte ich allerdings auch nicht mehr lesen wollen. Aber: „Wenn die Hoffnung stirbt, geht's" bei Peng „trotzdem weiter", und das ist gut so. Weil der Autor auch von den Recherchen zu den Aktionen erzählt, habe ich beim Lesen einiges gelernt und mich an anderes erinnert. Nur ein paar Beispiele: Als Peng auf der *re:publica* vier angebliche Google-Produkte von angeblichen Google-Managern präsentieren ließ, die die Metamorphose vom „freundliche[n], progressive[n] Bullerbü-Unternehmen" zum „Teil des staatlich-industrielle[n]

Überwachungskomplexes“ (Seite 84) erhellen sollten, habe ich einen kleinen Einblick in die Marketing-Strategie bei Produktnamen erhalten. Peng gab den Produkten

> *„vertrauenerweckende Namen: Google Trust, Google Bee, Google Hug und zum Abschluss Google Bye. Alles ungefährlich und dahergekumpelt.“ (Seite 96)*

Im Bericht über den *Hack* eines Science-Slam *(Slam Shell),* mit dem „der Ölkonzern Shell kommunikativ begrünt“ (Seite 77) werden sollte, habe ich von der PR-Agentur *Burson-Marsteller* erfahren, die

> *„auch Facebook, Union Carbide, Monsanto, aber auch Diktator_innen wie Nicolae Ceauşescu in Rumänien oder die argentinische Militärjunta beraten [hatte] – die Liste ihrer Kund:innen liest sich wie eine Armada der Umweltzerstörung, Menschenrechtsverletzung und gezielten Desinformation.“ (Seite 77)*

Was Waffenexporte angeht, habe ich wahrscheinlich mehr vergessen als ich je wusste. Peters erinnert mich:

> *„Alle paar Jahre kommen Skandale auf, in denen Politiker:innen geschmiert werden, in den illegale Exporte in Konfliktregionen bekannt werden, Verteidigungsminister wechseln nach ihrer Amtszeit sogar ganz offiziell in den Vorstand der Unternehmen.“ (Seite 107)*

Mir kommen die Kleinwaffen-Exporte von Heckler & Koch nach Mexiko mit den unbeschreiblichen Versehen/Vertuschungen/Fälschungen wieder hoch. Peters erzählt ab Seite 126 vom erfolgreichen Hack, und nebenbei berichtet er über den Ausgang der Verfahren gegen die Beschäftigten, mit skandalös niedrigen Strafen.

Bei der Aktion *Vattenfall übernimmt Verantwortung* konnte ich lesen, welche Medien mutmaßlich „mit Vattenfall im Bett“ (Seite 85) waren und welche Abgeordneten sich die gefakte Pressemitteilung dazu begeistert ans Revers hefteten. Und dann noch, wie der tschechische Konzern heißt, der Vattenfalls Kraftwerke und Kohlegruben in der Lausitz tatsächlich gekauft hat. Peters erzählt vom späteren Treffen mit dem Konzernleiter, der andeutet, man könne *Peng!* wegen zahlreicher markenrechtlicher Vergehen auf der Website zu diesem Hack anzeigen. Ein hübsches Beispiel von Peters' unterhaltsamem Stil:

> *„Das hatte unsere Medienanwältin auch bereits gesagt, aber das war mir egal: ‚Ich würde mich sehr freuen, gegen Sie ein Gerichtsverfahren zu führen', antwortete ich ihm, ‚in dem Sie ‚Vattenfall übernimmt Verantwortung' wegklagen möchten. Obendrein, wenn meine Verteidigung darin bestehen wird, dass es sich bei so einer Aussage nur um einen Fall von Kunstfreiheit handeln kann, da sie offensichtlich fernab der Realität ist.“ (Seite 93)*

Peng!

Gute Ideen, spannende Infos, kluge Gedanken und angenehm flapsig geschrieben. Ich kann es wärmstens empfehlen! Wer wenig Zeit zum Lesen von Büchern hat, sollte wenigstens mal auf die Website von Jean Peters gucken: Auf jeanpeters.de/liste finden sich alle Videos und Texte zu den Aktionen und Recherchen.

Anmerkung

1 *Schade, dass Bündnis 90/Die Grünen das nicht gelesen hatten, bevor sie in ihrem Wahlprogramm für ein Verbot der Großwildjagd in anderen Ländern stimmten. Dann hätten sie sich den Vorwurf neo-kolonialen Denkens erspart.*

Verlagsinformation

Rolf Gössner: Datenkraken im öffentlichen Dienst. „Laudatio“ auf den präventiven Sicherheits- und Überwachungsstaat

Der Jurist, Publizist und Bürgerrechtler Rolf Gössner legt sein neues Buch *Datenkraken im öffentlichen Dienst* vor – eine „Laudatio“ auf den präventiven Sicherheits- und Überwachungsstaat. Das Buch erscheint im PapyRossa Verlag (Köln) – wenige Monate nachdem der Autor am Ende eines 15-jährigen Gerichtsverfahrens endgültig über den Inlandsgeheimdienst „Verfassungsschutz“ gesiegt hat. Das Bundesverwaltungsgericht hat Gössners vier Jahrzehnte währende Dauerüberwachung rechtskräftig für unverhältnismäßig und grundrechtswidrig erklärt und ihn damit endgültig rehabilitiert. Der Autor stand nicht zuletzt auch wegen seiner fundierten Kritik an der Politik der„Inneren Sicherheit“ – wie er sie auch in diesem Buch übt und ausführt – unter staatlicher Langzeitbeobachtung des „Verfassungsschutzes“. So bleibt nur zu hoffen, dass ihn das höchstrichterliche Urteil auch in Hinblick auf den staats- und gesellschaftskritischen Inhalt des neuen Buches vor weiteren geheimdienstlichen Nachstellungen und Ausforschungen schützt.

Rolf Gössner
Datenkraken im öffentlichen Dienst. „Laudatio“ auf den präventiven Sicherheits- und Überwachungsstaat.
Mit Gastbeiträgen von Gerhart Baum, Sabine Leutheusser-Schnarrenberger und Heribert Prantl.
PapyRossa Verlag (Köln), Neue Kleine Bibliothek 297, 2021
366 Seiten
Preis € 19.90
ISBN 978-3-89438-753-2

Das Buch zeichnet den bundesdeutschen Weg in den präventiv-autoritären Sicherheits- und Überwachungsstaat nach – und zwar anhand der BigBrotherAwards, auch als „Oscars für Datenkraken" bekannt. Jährlich werden diese Negativpreise an die größten Datenfrevler verliehen: so auch an Regierungen, Politiker:innen, Ministerien und Sicherheitsbehörden. Deren „Antiterrorpolitik" und „Sicherheitsgesetze", Überwachungs- und Aufrüstungsmaßnahmen sind Meilensteine auf dem Weg einer fatalen Entwicklung im Namen der Sicherheit – aber mit Sicherheit auf Kosten der Freiheit. Diese Entwicklung zeichnen die kritisch pointierten „Laudationes" des Bürgerrechtlers Rolf Gössner nach, die er von 2000 bis 2020 gehalten hat. Ein ausführlicher Analyseteil ordnet die „ausgezeichneten" Fälle in die Geschichte Innerer Sicherheit ein und fragt zudem nach Folgen und Gefahren von Demokratie und Grundrechtsbeschränkungen im Zuge der Corona-Krise.

Rolf Gössner, *Dr. iur., *1948, Jurist und Autor zahlreicher Publikationen zum Themenspektrum Innere Sicherheit, Bürgerrechte und demokratischer Rechtsstaat. Kuratoriumsmitglied der Internationalen Liga für Menschenrechte, Mitherausgeber des Grundrechte-Reports (Fischer-TB) und der Zweiwochenschrift für Politik / Wirtschaft / Kultur Ossietzky sowie 2000 bis 2020 Mitglied der Jury zur Verleihung des Negativpreises BigBrotherAward. Für seine Bürgerrechtsarbeit ist er mehrfach ausgezeichnet worden.*

Grundrechte-Report 2021

Ungleiche Freiheiten und Recht in der Krise

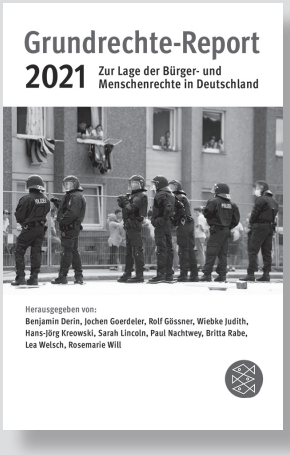
26. Mai 2021 – Der diesjährige Grundrechte-Report beschäftigt sich schwerpunktmäßig mit den Grundrechtseingriffen während der Covid-19 Pandemie. Wie der Bericht zeigt, treffen solche Einschränkungen besonders die schwächsten und vulnerabelsten Gruppen in der Gesellschaft.

Heute erscheint der neue Grundrechte-Report unter dem Titel *Ungleiche Freiheiten und Rechte in der Krise*. Mitherausgeberin **Sarah Lincoln**, Juristin bei der Gesellschaft für Freiheitsrechte, kommentiert für die Redaktion: „Der diesjährige Grundrechte-Report zeigt, wie zahlreich die Grundrechtsverletzungen und -einschränkungen im letzten Jahr waren. Mit unserem *Alternativen Verfassungsschutzbericht* legen wir als Grund- und Menschenrechtsorganisationen in Deutschland den Finger in die Wunde. Die Bundesregierung muss sich einigen Aufgaben stellen: Von grundrechtskonformer Pandemiebekämpfung über Respekt vor digitaler Privatsphäre zu zukunftstauglichem Klimaschutz und rassismusfreiem staatlichen Handeln."

Prof. Dr. **Naika Foroutan**, Professorin für Integrationsforschung und Gesellschaftspolitik an der Humboldt-Universität zu Berlin, stellt den Grundrechte-Report bei der Pressekonferenz vor und resümiert mit Blick auf die Erfahrungen im letzten Jahr: „Einschränkungen von Grundrechten treffen meist die schwächsten und vulnerabelsten Gruppen in unserer Gesellschaft. Sie können sich am wenigsten dagegen wehren. Ungleiche Rechte spiegeln daher auch den strukturellen Rassismus in diesem Land."

Dies zeigt sich unter anderem an den haftähnlichen Kollektivquarantänen, die in Sammelunterkünften für Geflüchtete verhängt wurden. Hiervon berichtet **Kawe Fatehi**, der 2019 als kurdischer Aktivist vor politischer Verfolgung aus dem Iran nach Deutschland flüchtete: „Als ich am Morgen des 27. März 2020 aufwachte, war die Zentrale Aufnahmestelle für Asylbewerber in Halberstadt von Polizisten umstellt. Fünf Wochen standen wir unter kollektiver Quarantäne, hunderte Menschen auf engem Raum und ohne jeglichen Schutz vor Ketteninfektionen. Alle hatten Angst – zu Recht, denn auch ich wurde nach zweieinhalb Wochen Quarantäne positiv getestet."

Das Konzept der „Clankriminalität" wird im diesjährigen Report in einem ausführlichen Beitrag kritisch beleuchtet. Wie **Mohammed Chahrour** von der Initiative *Kein Generalverdacht* feststellt:



Benjamin Derin, Jochen Goerdeler, Rolf Gössner, Wiebke Judith, Hans-Jörg Kreowski, Sarah Lincoln, Paul Nachtwey, Britta Rabe, Lea Welsch, Rosemarie Will (Hrsg.)
Grundrechte-Report 2021 – Zur Lage der Bürger- und Menschenrechte in Deutschland
Fischer Taschenbuch Verlag, Frankfurt/M., Mai 2021
267 Seiten
Preis € 12,00
ISBN 978-3-596-70622-8

„Sippenhaft und Kollektivschuld bleiben 2021 Bestandteil der gesellschaftlichen Realität für viele Menschen. Das Versprechen des Rechtsstaats wird bei ethnischen Minderheiten und sozial benachteiligten Gruppen nicht eingelöst: Vor dem Gesetz sind nicht alle gleich."

Neben diesen Themen beleuchtet der diesjährige Grundrechte-Report die Einschränkungen der Versammlungsfreiheit während der Pandemie, die Zumutungen der Coronakrise für Beschäftigte im Gesundheitssektor, die prekären Bedingungen in Schlachtbetrieben und die ungleichen Auswirkungen der Pandemie im Bildungsbereich. Daneben wirft der Report Schlaglichter auf Themen wie digitale Rechte und Vorratsdatenspeicherung, die Verfassungsbeschwerden zum Klimaschutz und den *Cum-Ex*-Steuerskandal.

Seit mehr als zwanzig Jahren erscheint der „Grundrechte-Report: Zur Lage der Bürger-und Menschenrechte in Deutschland". Die 43 Einzelbeiträge im 25. Grundrechte-Report widmen sich aktuellen Gefährdungen der Grundrechte und zentraler Verfas-

sungsprinzipien anhand konkreter Fälle des Jahres 2020. Der alternative Verfassungsschutzbericht analysiert und kritisiert Entscheidungen von Parlamenten, Behörden und Gerichten, aber auch von Privatunternehmen. Der Report wird von zehn Bürgerrechtsorganisationen herausgegeben.

Die Aufzeichnung der Veranstaltung zur Vorstellung des Grundrechte-Reports 2021 ist unter https://www.fiff.de/veranstaltungen/grundrechtereport2021 zu finden.

Der Grundrechte-Report 2021 ist ein gemeinsames Projekt von: Humanistische Union, vereinigt mit der Gustav Heinemann-Initiative • Bundesarbeitskreis Kritischer Juragruppen • Internationale Liga für Menschenrechte • Komitee für Grundrechte und Demokratie • Neue Richtervereinigung • PRO ASYL • Republikanischer Anwältinnen-und Anwälteverein • Vereinigung Demokratischer Juristinnen und Juristen • Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung • Gesellschaft für Freiheitsrechte

Wissenschaft & Frieden 2/2021: Völkerrecht in Bewegung. Von Krisen, Kritik und Erneuerung

Wie alle Rechtsbereiche entwickelt sich auch das Völkerrecht und mit ihm seine Institutionen. Manchenorts herrscht Stillstand, andernorts Aufbruchstimmung – im Gesamtblick kein eindeutiges Stimmungsbild. Ausgabe 2/2021 von W&F nähert sich aktuellen Entwicklungen im Völkerrecht.

Unsere Autor:innen fragen: Wie können zivilgesellschaftliche Akteur:innen Menschenrechtsverstöße oder Kriegsverbrechen verfolgen lassen? Welchen Status hat eigentlich die Natur im Völkerrecht? Was sind die Erfolge und Misserfolge des „Weltrechtsprinzips" in Deutschland? Kann ein Verfahren wegen der Gesundheitspolitik eines Staates vor dem Internationalen Strafgerichtshof gelingen? W&F wagt eine Zwischenbilanz und den Ausblick auf weitere Entwicklungen.

Daneben findet sich in dieser Ausgabe ein Beitrag zur Rolle von Umwelt und nachhaltiger Entwicklung im Konflikt und der Konfliktbearbeitung in Ruanda sowie ein kurzer Überblicksbeitrag zum Konfliktgeschehen in 2020. Gastkommentar und Presseschau behandeln die Konsequenzen der Abzugsperspektive internationaler Kräfte aus Afghanistan, sowie die (Miss-)Erfolge des Kriegseinsatzes. Im Forum finden sich spannende Rezensionen zu Omri Boehm, Judith Butler und Ullrich Hahn sowie Konferenzberichte aus dem ersten Quartal.

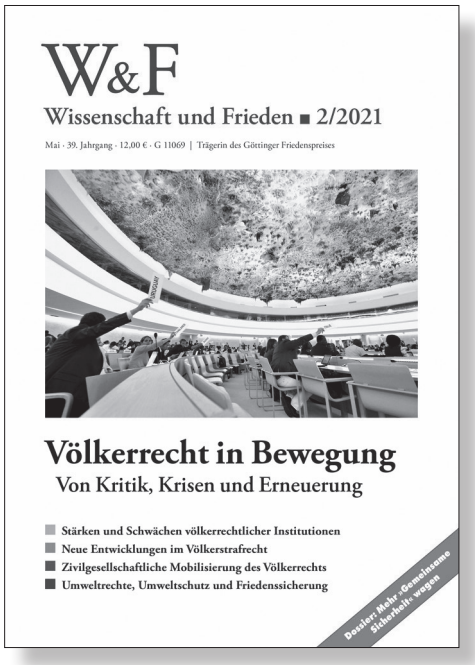
Dossier 92

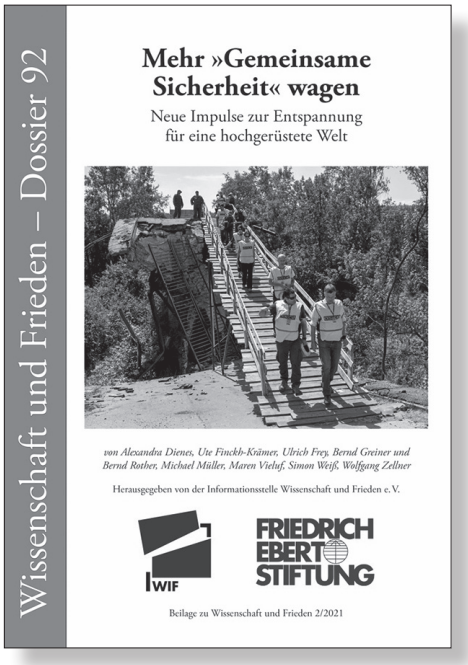
Mehr „Gemeinsame Sicherheit" wagen. Neue Impulse zur Entspannung für eine hochgerüstete Welt

Im Angesicht der weltweit weiter wachsenden Spannungen und der Bereitschaft der Staaten, vor allem auf militärische Abschreckungslogik zu setzen, will dieses Dossier ein Plädoyer sein: für mehr »Gemeinsame Sicherheit«, für eine (selbst)kritische (Rück-) Besinnung auf Werte, Begriffe und Konzepte der Entspannungspolitik und für den immer wieder erneuten Anlauf, Friedenspolitik und Entspannung zu suchen. Ein gewichtiges Plädoyer, nicht nur im Wahljahr 2021.

Mit Impulsen von Alexandra Dienes, Ute Finckh-Krämer, Ulrich Frey, Bernd Greiner und Bernd Rother, Michael Müller, Maren Vieluf, Simon Weiß und Wolfgang Zellner.

W&F 2/21 | August | 64 Seiten | 12 € (print) / 9 € (epub) | *wissenschaft-und-frieden.de*





FIfF e.V.

Im FIfF haben sich rund 700 engagierte Frauen und Männer aus Lehre, Forschung, Entwicklung und Anwendung der Informatik und Informationstechnik zusammengeschlossen, die sich nicht nur für die technischen Aspekte, sondern auch für die gesellschaftlichen Auswirkungen und Bezüge des Fachgebietes verantwortlich fühlen. Wir wollen, dass Informationstechnik im Dienst einer lebenswerten Welt steht. Das FIfF bietet ein Forum für eine kritische und lebendige Auseinandersetzung – offen für alle, die daran mitarbeiten wollen oder auch einfach nur informiert bleiben wollen.

Vierteljährlich erhalten Mitglieder die Fachzeitschrift FIfF-Kommunikation mit Artikeln zu aktuellen Themen, problematischen Entwicklungen und innovativen Konzepten für eine verträgliche Informationstechnik. In vielen Städten gibt es regionale AnsprechpartnerInnen oder Regionalgruppen, die dezentral Themen bearbeiten und Veranstaltungen durchführen. Jährlich findet an wechselndem Ort eine Fachtagung statt, zu der TeilnehmerInnen und ReferentInnen aus dem ganzen Bundesgebiet und darüber hinaus anreisen. Darüber hinaus beteiligt sich das FIfF regelmäßig an weiteren Veranstaltungen, Publikationen, vermittelt bei Presse- oder Vortragsanfragen ExpertInnen, führt Studien durch und gibt Stellungnahmen ab etc. Das FIfF kooperiert mit zahlreichen Initiativen und Organisationen im In- und Ausland.

FIfF-Mailinglisten

FIfF-Mailingliste
An- und Abmeldungen an:
http://lists.fiff.de/mailman/listinfo/fiff-L
Beiträge an: *fiff-L@lists.fiff.de*

FIfF-Mitgliederliste
An- und Abmeldungen an:
http://lists.fiff.de/mailman/listinfo/mitglieder

Mailingliste Videoüberwachung:
An- und Abmeldungen an:
http://lists.fiff.de/mailman/listinfo/cctv-L
Beiträge an: *cctv-L@lists.fiff.de*

FIfF online

Das ganze FIfF
www.fiff.de
Twitter FIfF e.V. – *@FIfF_de*

Cyberpeace
cyberpeace.fiff.de
Twitter Cyberpeace – *@FIfF_AK_RUIN*

Faire Computer
blog.faire-computer.de
Twitter Faire Computer – *@FaireComputer*

Mitglieder-Wiki
https://wiki.fiff.de

FIfF-Beirat

Ute Bernhardt (Berlin); **Peter Bittner** (Kaiserslautern); **Dagmar Boedicker** (München); Dr. **Phillip W. Brunst** (Köln); Prof. Dr. **Wolfgang Coy** (Berlin); Prof. Dr. **Wolfgang Däubler** (Bremen); Prof. Dr. **Christiane Floyd** (Berlin); Prof. Dr. **Klaus Fuchs-Kittowski** (Berlin); Prof. Dr. **Michael Grütz** (München); Prof. Dr. **Thomas Herrmann** (Bochum); Prof. Dr. **Wolfgang Hesse** (München); Prof. Dr. **Wolfgang Hofkirchner** (Wien); Prof. Dr. **Eva Hornecker** (Weimar); **Werner Hülsmann** (München); **Benjamin Kees** (Berlin); **Ulrich Klotz** (Frankfurt am Main); Prof. Dr. **Klaus Köhler** (Mannheim); Prof. Dr. **Jochen Koubek** (Bayreuth); Prof. Dr. **Herbert Kubicek** (Bremen); Dr. **Constanze Kurz** (Berlin); Prof. Dr**. Klaus-Peter Löhr** (Berlin); Prof. Dr. **Dietrich Meyer-Ebrecht** (Aachen); **Werner Mühlmann** (Calau); Prof. Dr. **Frieder Nake** (Bremen); Prof. Dr. **Rolf Oberliesen** (Paderborn); Prof. Dr. **Arno Rolf** (Hamburg); Prof. Dr. **Alexander Rossnagel** (Kassel); **Ingo Ruhmann** (Berlin); Prof. Dr. **Gerhard Sagerer** (Bielefeld); Prof. Dr. **Gabriele Schade** (Erfurt); **Ralf E. Streibl** (Bremen); Prof. Dr. **Marie-Theres Tinnefeld** (München); Dr. **Gerhard Wohland** (Mainz); Prof. Dr. **Eberhard Zehendner** (Jena)

FIfF-Vorstand

Stefan Hügel (Vorsitzender) – Frankfurt am Main
Rainer Rehak (stellv. Vorsitzender) – Berlin
Michael Ahlmann – Kiel / Blumenthal
Maximilian Hagner – Jena
Alexander Heim – Berlin
Sylvia Johnigk – München
Prof. Dr. **Hans-Jörg Kreowski** – Bremen
Kai Nothdurft – München
Jens Rinne – Mannheim
Prof. Dr. **Britta Schinzel** – Freiburg im Breisgau
Ingrid Schlagheck – Bremen
Anne Schnerrer – Berlin
Prof. Dr. **Werner Winzerling** – Fulda

FIfF-Geschäftsstelle

Ingrid Schlagheck (Geschäftsführung) – Bremen
Philip Love – Bremen

Impressum

Herausgeber	Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e. V. (FIfF)
Verlagsadresse	FIfF-Geschäftsstelle Goetheplatz 4 D-28203 Bremen Tel. (0421) 33 65 92 55 *fiff@fiff.de*
Erscheinungsweise	vierteljährlich
Erscheinungsort	Bremen
ISSN	0938-3476
Auflage	1 200 Stück
Heftpreis	7 Euro. Der Bezugspreis für die FIfF-Kommunikation ist für FIfF-Mitglieder im Mitgliedsbeitrag enthalten. Nichtmitglieder können die FIfF-Kommunikation für 28 Euro pro Jahr (inkl. Versand) abonnieren.
Hauptredaktion	Dagmar Boedicker, Stefan Hügel (Koordination), Sylvia Johnigk, Hans-Jörg Kreowski, Dietrich Meyer-Ebrecht, Ingrid Schlagheck
Schwerpunktredaktion	Eberhard Zehendner mit Unterstützung von Christina B. Class, Dagmar Boedicker, Kai Nothdurft, Michael Ahlmann, Sylvia Johnigk
V.i.S.d.P.	Stefan Hügel
Retrospektive	Beiträge für diese Rubrik bitte per E-Mail an *redaktion@fiff.de*
Lesen, SchlussFIfF	Beiträge für diese Rubriken bitte per E-Mail an *redaktion@fiff.de*
Layout	Berthold Schroeder, München
Cover	Christian Wiegert, Bauhaus-Universität Weimar
Druck	Meiners Druck, Bremen Heftinhalt auf 100 % Altpapier gedruckt.

KLIMAneutral produziert

Die FIfF-Kommunikation ist die Zeitschrift des „Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e. V." (FIfF). Die Beiträge sollen die Diskussionen unter Fachleuten anregen und die interessierte Öffentlichkeit informieren. Namentlich gekennzeichnete Artikel geben die jeweilige Autor.innen-Meinung wieder.

Die FIfF-Kommunikation ist das Organ des FIfF und den politischen Zielen und Werten des FIfF verpflichtet. Die Redaktion behält sich vor, in Ausnahmefällen Beiträge abzulehnen.

Wichtiger Hinweis: Wir bitten alle Mitglieder und Abonnent:innen, Adressänderungen dem FIfF-Büro möglichst umgehend mitzuteilen.

Aktuelle Ankündigungen

(mehr Termine unter *www.fiff.de*)

FIfF-Kommunikation

4/2021 KI zieht in den Krieg
Hans-Jörg Kreowski, Aaron Lye u. a.
Redaktionsschluss: 5. November 2021

Zuletzt erschienen:

2/2020 Gesundheitswesen im Datenrausch
3/2020 Technologie und Ökologie
4/2020 Digitalisierung in der Bildung
1/2021 Datenschutz Usability Barrierefreiheit Informationssicherheit

---

W&F – Wissenschaft & Frieden

2/20 Frieden begreifen
3/20 Der kranke Planet
4/20 Umwelt, Klima Konflikt – Krieg oder Frieden mit der Natur?
1/21 »Friedensmacht« EU? – Zwischen Diplomatie und Militarisierung?
2/21 Völkerrecht in Bewegung. Von Krisen, Kritik und Erneuerung
3/21 Frieden lernen, aber wie? – Aktuelle Fragen der Friedenspädagogik

---

vorgänge – Zeitschrift für Bürgerrechte und Gesellschaftspolitik

#228 Wohnen als soziales Grundrecht
#229 Sterbehilfe
#230 30 Jahre Deutsch-Deutsche Wiedervereinigung
#231/232 Zwei Jahre Datenschutz-Grundverordnung

DANA – Datenschutz-Nachrichten

1/20 Gesundheitsdaten – Geheim oder Gemeingut?
2/20 E-Payment
3/20 E-Government – Datenschutz in öffentlichen Stellen
4/20 Mobilität
1/21 Biometrie
2/21 Bildung

Das FIfF-Büro

Geschäftsstelle FIfF e. V.
Ingrid Schlagheck (Geschäftsführung)
Philip Love
Goetheplatz 4, D-28203 Bremen
Tel.: (0421) 33 65 92 55, Fax: (0421) 33 65 92 56
E-Mail: fiff@fiff.de
Die Bürozeiten finden Sie unter *www.fiff.de*

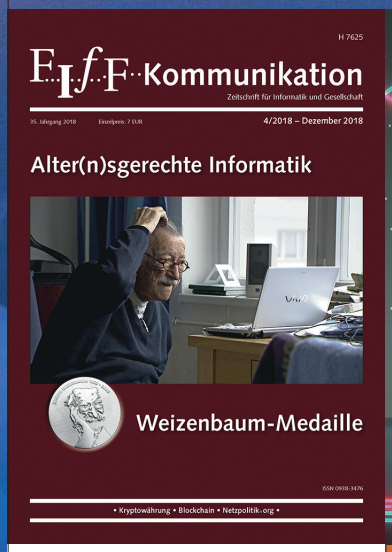
Bankverbindung
Bank für Sozialwirtschaft (BFS) Köln
Spendenkonto:
IBAN: DE79 3702 0500 0001 3828 03
BIC: BFSWDE33XXX

Kontakt zur Redaktion der FIfF-Kommunikation:
redaktion@fiff.de

Viermal im Jahr geben wir die FIfF-Kommunikation heraus. Sie entsteht durch viel ehrenamtliche, unbezahlte Arbeit. Doch ihre Herstellung kostet auch Geld – Geld, das wir nur durch Eure Mitgliedsbeiträge und Spenden aufbringen können.

Auch unsere weitere politische Arbeit kostet Geld für Öffentlichkeitsarbeit, Aktionen und Organisation. Unsere jährlich stattfindende FIfF-Konferenz, der Weizenbaum-Preis, weitere Publikationen und die Kommunikation im Web.

Bitte unterstützt das FIfF mit einer Spende.



Das FIfF bittet um Eure Unterstützung

Spendenkonto:
Bank für Sozialwirtschaft (BFS) Köln,
IBAN: DE79 3702 0500 0001 3828 03
BIC: BFSWDE33XXX