H 7625

FIfF Kommunikation

Zeitschrift für Informatik und Gesellschaft

36. Jahrgang 2019 Einzelpreis: 7 EUR 2/2019 – Juni 2019

Brave New World

Gestaltungsfreiheiten und Machtmuster soziotechnischer Systeme – 2

ISSN 0938-3476

• Weizenbaum Studienpreise • Faktencheck zu Rezo • Ein Jahr DSGVO •

FIfF Kommunikation

Zeitschrift für Informatik und Gesellschaft

Titelbild: Motiv des Tagungsplakats der FIfFKon 2018

Inhalt

Ausgabe 2/2019

inhalt

Editorial

Dies ist die zweite Ausgabe in diesem Jahr, die wiederum Beiträge zur FIfF-Konferenz 2018 – *Brave New World* – enthält. Das sind zunächst vier weitere Vorträge der Tagung, die wir in der Redaktion verschriftlicht haben. *Florian Schumacher* sprach über *Cybersicherheit in der Digitalisierung*, die eine Herausforderung für Staat, Wirtschaft und Gesellschaft darstellt. *Rainer Mühlhoff* stellte dar, wie die heutigen Methoden des *Usability Experience Design* (UX) durch Nudging, Massendaten und versiegelte Oberflächen zur *Digitalen Entmündigung* der Benutzerinnen und Benutzer führt. *Aljoscha Burchardt*, *Constanze Kurz* und *Karen Ullrich* diskutierten über Künstliche Intelligenz und ihre theoretischen Grenzen, praktischen Möglichkeiten und den darüber geführten politischen Diskurs. Ihre Podiumsdiskussion hatte auch aktuellen Bezug – in der Woche vor der Konferenz hatte sich im Deutschen Bundestag die Enquête-Kommission zur Künstlichen Intelligenz konstituiert, von der sicherlich an dieser Stelle noch zu lesen sein wird. Im letzten Beitrag dieses Abschnitts kommentieren *Kirsten Bock* und *Malte Engeler* ihre *Reise durch die (Un-) Tiefen des juristischen Feuilletons* und ziehen eine *launige Bilanz der Datenschutz-Grundverordnung*, die bei der Konferenz gerade mal seit vier Monaten geltendes Recht war.

Erstmals verliehen wir bei dieser Konferenz den bisherigen FIfF-Studienpreis als *Weizenbaum-Studienpreis*. Preisträger waren *Leon Kaiser* mit seiner Arbeit *Vulnerable Systems. The Quantification of Affect in an Experimental Blockchain Pilot-Project for Financial Transactions Management for Refugees*, *Severin Engelmann* mit *The Digital Dimensions of Personal Identity* und *Nico Lück* mit *Künstliche Intelligenz und Rüstungskontrolle. Der Einsatz maschinellen Lernens in Waffensystemen und Verifikationsmaßnahmen*. Einen Sonderpreis verliehen wir an *Jörg Pohle*. Dessen Arbeit *Datenschutz und Technikgestaltung* hat aus unserer Sicht große Bedeutung für die anstehenden Debatten zu Ziel und Bedeutung des Datenschutzes. Klare Leseempfehlung – für alle prämierten Arbeiten.

Während wir noch die FIfF-Konferenz 2018 inhaltlich aufbereiten, läuft die Vorbereitung der FIfF-Konferenz 2019 bereits auf Hochtouren. Freut Euch auf *Künstliche Intelligenz als Wunderland*, vom 2.-24. November 2019 in Bremen.

Großen Aufruhr in der politschen Szene verursachte von den Wahlen zum Europäischen Parlament der Youtuber Rezo (@rezomusic). In einem rund einstündigen Video analysierte er die Regierungspolitik und kam zu ernüchternden Ergebnissen. Er forderte seine ZuseherInnen auf, nicht SPD, nicht CDU/CSU und selbstverständlich auch nicht AfD zu wählen. Besonders griff er in dem Video die Politik der CDU an – unter anderem die Militär- und die Klimapolitik. Einige Tage später legte er, gemeinsam mit ca. 90 Kolleginnen und Kollegen nach, und veröffentlichte ein weiteres Video, in dem erneut dazu aufgerufen wurde, die genannten Parteien nicht zu wählen.

Erwartungsgemäß schäumte von allem die hauptsächlich angegriffene CDU. Es gelang ihr aber nicht, Rezo überzeugend zu widerlegen. Das 11-seitige Papier, dass sie veröffentlichte – nachdem sie ein bereits angekündigtes Video zurückgezogen hatte – hatte wenig Substanz. Wir haben uns den Teil des Videos und der Antwort der CDU besonders angeschaut und kommentiert, der sich im wesentlichen mit dem militärischen Einsatz von Drohnen befasste. Die dabei entstandene Presseerklärung ist in dieser Ausgabe enthalten.

Von der Enquête-Kommission für Künstliche Intelligenz war schon die Rede. Hans-Jörg Kreowski war als Sachverständiger für das Thema KI und äußere Sicherheit eingeladen und berichtet in dieser Ausgabe darüber. Künstliche Intelligenz – vor allem in Form das Machine Learning, in dem momentan einige Erfolge zu verzeichnen sind – ist zweifellos auch darüber hinaus ein Thema, das uns weiter beschäftigen wird, und so ist es bedauerlich, „… dass ihre Arbeit", wie Hans-Jörg Kreowski feststellt, „weitgehend hinter verschlossenen Türen stattfindet und dass die Öffentlichkeit nur völlig unzulänglich einbezogen ist. Die Kommission verpasst die Chance eines breiten und offenen gesellschaftlichen Diskurses. Schade."

Die Rubrik *netzpolitik.org* enthält diesmal vier Beiträge: eine Bilanz der europäischen Netzpolitik der letzten fünf Jahre, ein Beitrag über die Nutzung von Künstlicher Intelligenz, um die Moderationsprobleme bei Facebook zu lösen – und die Probleme damit –, einen Kommentar zur Europawahl, die aus Sicht von *Markus Beckedahl* im Internet entschieden wurde und bei der die Urheberrechtsreform und die Fridays-for-Future-Proteste eine wichtige Rolle gespielt haben, und Stimmen von zwölf Vertreterinnen und Vertretern der Zivilgesellschaft zu einem Jahr Datenschutz-Grundverordnung.

Dagmar Boedicker hat sich den Band *Das metrische Wir – über die Quantifizierung des Sozialen* von *Steffen Mau* vorgenommen und rezensiert.

Erlaubt mir zuletzt – weil ich es gerade aus dem Briefkasten gefischt habe – eine kleine Werbeeinblendung. Im November war das FIfF Teil des Trägerkreises der Konferenz *Bits & Bäume* an der Technischen Universität Berlin. Jetzt ist das Buch zur Konferenz fertig: *Was Bits und Bäume verbindet – Digitalisierung nachhaltig gestalten*. Der Band enthält auch einige Beiträge von FIfF-Aktiven, wurde herausgegeben von *Anja Höfner* und *Vivian Frick* und ist im Oekom-Verlag erschienen. Dort kann der Band auch als E-Book heruntergeladen werden.

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

Stefan Hügel
für die Redaktion

Der Brief

Politische Umwälzungen

Liebe Leserinnen und Leser, liebe Mitglieder des FIfF.

Mit Spannung wurde die Wahl zum europäischen Parlament erwartet – und tatsächlich brachten sie die erwarteten Umwälzungen, mit möglicherweise weitreichenden Folgen für die politische Landschaft.

Verlierer sind zunächst die bisherigen „Volksparteien" – und hier beobachten wir möglicherweise das Ende eines politischen Konzepts. Volksparteien werden dafür gelobt, politische Strömungen breit zu integrieren. Dies geht aber auf Kosten der Transparenz: Politische Prozesse und Debatten, die eigentlich in der Öffentlichkeit stattfinden sollten, werden in die Parteien hinein und damit potenziell ins Hinterzimmer verlagert. Das hat jahrzehntelang funktioniert, da die Parteien (bzw. deren Führung) bevorzugten Zugriff auf Kommunikationsmittel – Fernsehen, Radio, Presse – hatten und damit die öffentlche Meinung dominieren konnten. Die politische Durchschlagskraft von Leserbriefen ist halt begrenzt. Doch das ist vorbei, wie exemplarisch das Video des Youtubers Rezo[1] und das darauffolgende Video einer ganzen Gruppe von Youtubern[2] zeigte – auf das die etablierten Parteien keine Antwort wussten. Im Gegenteil: Das erst angekündigte und dann zurückgezogene Video des Bundestagsabgeordneten Philipp Amthor löste zusätzlich Häme aus. Letztlich veröffentlichte die CDU ein Positionspapier[3]. Analysen dazu gab es z. B. von uns[4] und von Prof. Dr. Volker Quaschning vom Netzwerk Scientists for Future[5].

Aber Vorsicht! Auch wenn sich hier scheinbar neue Möglichkeiten öffentlcher Teilhabe an politischen Debatten auftun: Die Meinungsmacht hängt auch bei Youtube letztlich von den Ressourcen und finanziellen Möglichkeiten ab[6]. Es ist auch noch zu untersuchen, welchen Einfluss das Video tatsächlich auf das Wahlergebnis hatte.

Die etablierten Parteien schäumten[7] – und setzen ihre Kampagnen gegen „Fake News" fort. Doch Falschmeldungen hat es immer gegeben – und sie stehen nicht selten mit einzelnen Presseerzeugnissen, beispielweise eines großen Berliner Zeitungsverlags[8], in Verbindung[9]. Das war bereits 1968 so, mit den bekannten Folgen[10], und es hat sich wenig daran geändert. Vor diesem Hintergrund ist es ein wenig dürftig, wenn Rezo jede kleine Ungenauigkeit vorgehalten und mit persönlichen Angriffen seine Integrität in Zweifel gezogen wurde. Es wäre zu wünschen, bei Bierzeltreden nicht nur bayerischer PolitikerInnen die gleichen Maßstäbe anzusetzen. Es ist auch erstaunlich, wenn beispielsweise der Chefredakteur eines der oben angedeuteten Presseerzeugnisse in der Debatte um den Klimawandel und der dafür vorgeschlagenen Umstellung auf Elektrofahrzeuge mit dem Hinweis begegnet, Elektrofahrzeuge hätten keine Seele[11] – und dafür nicht schallend ausgelacht wird[12].

Erstes Opfer der Europawahlen ist Andrea Nahles, deren Parteikarriere offenbar zu Ende ist. Doch die gesamte SPD scheint in einen Strudel gerissen worden zu sein, aus dem sie nicht mehr entkommen kann – oder es überhaupt nicht mehr will? Jedenfalls ist kein Umsteuern erkennbar; tonangebend scheint immer noch der Seeheimer Kreis zu sein, und es scheint weiterhin die Meinung vorzuherrschen, man könne einfach so weitermachen wie bisher[13] – nachdem man in den Umfragen bei 12 % angekommen ist.

Große Gewinner der Europawahlen – was sich in den darauf folgenden Umfragen noch verstärkt fortsetzte – sind die Grünen[14]. Man kann wohl annehmen, dass auch die Fridays-for-Future-Bewegung mit ihrem Einsatz für den Klimaschutz dazu beigetragen hat. Von den Grünen wird von allen im Bundestag vertretenen Parteien wohl am meisten erwartet, dass sie dem drohenden Klimawandel mit effektiven Maßnahmen begegnen werden.

Doch die Grünen, bei aller nachvollziehbaren Freude über das Wahlergebnis, könnten dadurch in eine Zwickmühle geraten. Effektiver Klimaschutz ist – nach den Versäumnissen der letzten Jahrzehnte – wohl nicht mehr machbar ohne spürbare Einschnitte: beim Flugverkehr, bei der individuellen Motorisierung bis hin zur Ernährung. Der Aufschrei, als die Grünen vor der Bundestagswahl 2013 einen obligatorischen „Veggie-Day"[15] gefordert hatten, wird ihnen wohl noch in schmerzhafter Erinnerung sein. Der Vorschlag des Bundestagsabgeordneten Dieter Janiczek, die Anzahl der (günstigen) Flugreisen pro Person auf drei zu begrenzen, wurde auch bei den Grünen nicht gerade mit Wohlwollen aufgenommen[16]. Und schauen wir uns die real existierende grüne Politik in den Ländern an: Die Grün-geführte Landesregierung in Baden-Württemberg unterstützt nach wie vor den Bau des Bahnhofs Stuttgart 21, die Landesregierung klagte gegen Fahrverbote in Stuttgart[17], Ministerpräsident Kretschmann engagiert sich mit seinen Kollegen Weil und Söder für die Automobilindustrie[18]. In Hessen wird der weitere Ausbau des Flughafens Frankfurt vorangetrieben – unter einem grünen Wirtschaftsminister[19]. Wenig Mut macht auch die Zulassungsstatistik für Personenkraftwagen im Mai 2019 – gegenüber Mai 2018 sind die Zulassungszahlen für Sports Utility Vehicles (SUV) um 32,0 %, die Zulassungszahlen für Geländewagen um 22,8 % gestiegen[20].

Dass beide Landesregierungen auch bei der Frage von Überwachung, Datenschutz und Bürgerrechten höchst zweifelhaft agieren, sei hier nur der Vollständigkeit halber erwähnt[21].

2008 wurde in den Vereinigten Staaten Barack Obama zum Präsidenten gewählt. Er wurde fast wie ein Messias gefeiert – auch in Deutschland – und gleich zu Beginn seiner Amtszeit mit dem Friedensnobelpreis geehrt, in der Erwartung einer kommenden Friedenspolitik. Man muss wohl feststellen, dass er diese Erwartung – wie auch andere – nicht erfüllt hat. 2012, nach seinem zweiten Wahlsieg, schrieb ich an dieser Stelle:

> *„Nachdem er beim ersten Mal große Begeisterung auslöste und viele neue Wählerinnen und Wähler an die Urne lockte, scheint von dieser Begeisterung nicht viel*

übrig geblieben zu sein. Die Auswirkungen solcher Enttäuschung auf die Akzeptanz des demokratischen Systems sind heute kaum abzuschätzen.“[22]

I hate to say, I told you so, aber: Heute haben wir es mit einem US-Präsidenten Trump zu tun. Obama konnte die großen Erwartungen nicht erfüllen – und es ist nicht einmal klar, ob er es überhaupt wollte. Seine Politik konnte die Wählerinnen und Wähler nicht überzeugen; Hillary Clinton als Kandidatin für seine Nachfolge, die bei der Präsidentschaftswahl 2016 schon als Gewinnerin festzustehen schien, wurde dafür abgestraft.

Man stelle sich vor: eine Bundeskanzlerin Baerbock oder ein Bundeskanzler Habeck, der die hochgesteckten Erwartungen nicht erfüllen kann, und in einigen Jahren durch einen Bundeskanzler Meuthen oder eine Bundeskanzlerin Weidel abgelöst wird. Wir können nur hoffen, dass sich die Grünen ihrer riesigen Verantwortung sehr bewusst sind. Wir sollten dabei auch sehr genau nach Frankreich schauen: Wird womöglich Präsident Macron bei der nächsten Wahl durch Madame Le Pen ersetzt? Nicht auszudenken!

Generell stellt sich die Frage nach den politischen Linien, an denen künftige Debatten ausgerichtet sind. Die klassische Unterscheidung zwischen links und rechts scheint sich immer mehr aufzulösen. Nancy Fraser zieht die Linie zwischen progressivem Neoliberalismus – wirtschaftlich neoliberal und rückschrittlich, gesellschaftlich fortschrittlich – und dem reaktionären Rechtspopulismus[23]. Clinton vs. Trump, Macron vs. Le Pen – und Habeck vs. Meuthen?

Welche Auswirkungen dabei der Klimawandel letztlich hat, wenn seine Auswirkungen deutlicher werden, muss man sehen. Greta Thunberg sagte in ihrer Rede in Katowice:

„And if solutions within this system are so impossible to find, then maybe we should change the system itself.“[24]

Die Antwort, was das langfristig heißt, können wir von ihr fairerweise nicht verlangen. Aber irgendwer muss sie wohl geben.

Der Erfolg der PARTEI mit Martin Sonneborn und Nico Semsrott ist ein weiteres Indiz für die Erosion des demokratischen Systems, wie wir es kennen. Man mag die beiden als Kabarettisten schätzen – muss sich aber auch im Klaren sein, dass durch dieses Wahlverhalten und die Wahlaussagen der PARTEI das Parlament zusätzlich delegitimiert wird. Kann man machen – irgendwann muss aber auch hier jemand die Antwort geben, was an seine Stelle treten soll.

Zuletzt: Wir müssen damit rechnen, dass der Klimawandel, den die „Westliche Welt“ hauptsächlich verantwortet, zu einer massiven Zunahme der Migration führt – der globale Süden wird den Hauptteil der Folgen zu tragen haben. Dürren führen zu Bürgerkriegen und Bürgerkriege führen zur Flucht[25]. Doch dafür möchten wir anscheinend keine Verantwortung übernehmen. Der Anfang wurde bereits 1993 gemacht[26]. Gerade hat die „große“ Koalition, vielleicht als letztes Zucken, das „Geordnete-Rückkehr-Gesetz“ beschlossen[27]. Manche nennen es das „Hau-ab-Gesetz“[28]. Ob das Gesetzespaket einer verfassungsrechtlichen Prüfung standhält, muss sich zeigen – der Versuch, den Inhalt von Gesetzen durch besondere Kompliziertheit zu verschleiern, wie sie Bundesheimatminister Seehofer ankündigte, wird dabei hoffentlich ins Leere laufen[29]. Aber vielleicht ist es höchste Zeit, dass eine Regierung, die solche Gesetze beschließt, bald abgelöst wird.

Mit FIfFigen Grüßen

Stefan Hügel

Anmerkungen

1 *@rezomusic: Die Zerstörung der CDU, https://www.youtube.com/watch?v=4Y1lZQsyuSQ*
2 *@rezomusic et al.: Ein Statement von 90+ Youtubern, https://www.youtube.com/watch?v=Xpg84NjCr9c*
3 *CDU: Offene Antwort an Rezo: Wie wir die Sache sehen, https://www.cdu.de/artikel/offene-antwort-rezo-wie-wir-die-sache-sehen*
4 *FIfF e. V.: Das FIfF stützt und bestätigt die Aussagen über Drohneneinsätze der USA, die über die US-Airbase Ramstein in Deutschland koordiniert werden, Pressemitteilung vom 25. Mai 2019, https://www.fiff.de/presse/rezo-drohnen*
5 *Volker Quaschning: Faktencheck des Teils „Die Klimakrise“ der offenen Antwort der CDU an REZO vom 23.05.2019, https://www.volker-quaschning.de/artikel/2019-05_Stellungnahme-CDU/index.php*
6 *Auf die Risiken wies bereits vor einigen Jahren Evgeny Morozov (2011) hin: The Net Delusion. How not to liberate the World, London u. a.: Penguin Books*
7 *z. B. Paul Ziemiak, https://www.tagesspiegel.de/gesellschaft/medien/paul-ziemiak-reagiert-auf-youtuber-rezo-cdu-nennt-video-von-youtuber-gefaehrlich/24369318.html*
8 *Günter Wallraff (1977): Der Aufmacher: Der Mann, der bei BILD Hans Esser war. Köln: Kiepenheuer & Witsch; literarisch wurden die Auswirkungen dieser Form der Berichterstattung beispielsweise verarbeitet in Heinrich Böll (1974): Die verlorene Ehre der Katharina Blum. Köln: Kiepenheuer & Witsch*
9 *Alexander Sängerlaub, Miriam Meier, Wolf-Dieter Rühl (2017): Fakten statt Fakes. Verursacher und Verbreitungswege von Fake News im Bundestagswahlkampf 2017. Stiftung neue Verantwortung. https://www.stiftung-nv.de/sites/default/files/snv_fakten_statt_fakes.pdf*
10 *https://de.wikipedia.org/wiki/Außerparlamentarische_Opposition, https://de.wikipedia.org/wiki/Rudi_Dutschke*
11 *https://www.spiegel.de/kultur/tv/hart-aber-fair-mit-frank-plasberg-zur-klimakrise-sorry-wir-haben-keine-zeit-mehr-a-1259596.html*
12 *Dass Elektrofahrzeuge als Ersatz für Fahrzeuge, die durch Verbrennungsmotoren angetrieben werden, durchaus auch kritisch betrachtet werden, ist dem Autor selbstverständlich bewusst.*
13 *Scholz sieht SPD mit Chancen auf Kanzlerschaft: https://www.spiegel.de/politik/deutschland/olaf-scholz-sieht-spd-mit-chancen-auf-kanzlerschaft-a-1270931.html*
14 *z. B. https://twitter.com/Wahlrecht_de/status/1137361149501087744*
15 *https://de.wikipedia.org/wiki/Veggieday*
16 *Gerade AnhängerInnen der Grünen wird nachgesagt, auch im Vergleich zu AnhängerInnen anderer Parteien relativ häufig mit dem Flugzeug unterwegs zu sein. Dies als Argument gegen Klimaschutz ins Feld zu führen ist zwar albern, weist aber auf die Schwierigkeiten bei der Debatte hin: https://www.rbb-online.de/kontraste/archiv/kontraste-vom-21-03-2019/gruene-vielflieger.html*
17 *Landesregierung geht gegen Urteil zu Fahrverboten vor, https://www.spiegel.de/auto/aktuell/stuttgart-landesregierung-will-fahrverbote-fuer-dieselautos-verhindern-a-1163733.html*

18 *BPK über die „Zukunft der Autoindustrie" mit Markus Söder (CSU), Winfried Kretschmann (Grüne) & Stephan Weil (SPD), http://www.jungundnaiv.de/2019/06/07/bpk-ueber-die-zukunft-der-autoindustrie-mit-markus-soeder-csu-winfried-kretschmann-gruene-stephan-weil-spd/*

19 *Am Aschermittwoch ist für Al-Wazir nichts vorbei, https://www.faz.net/aktuell/rhein-main/frankfurter-flughafen-die-kehrtwende-der-gruenen-13432931.html*

20 *Neuzulassungsbarometer des Kraftfahrt-Bundesamts, aus dem auch hervorgeht, dass die Fahrzeugklasse SUV mit 20,3 % nur knapp hinter der Kompaktklasse an zweiter Stelle der Neuzulassungen liegt. Bei Geländewagen sind es 9,5 %: https://www.kba.de/DE/Statistik/Fahrzeuge/Neuzulassungen/MonatlicheNeuzulassungen/2019/201905_GImonatlich/201905_nzbaromter/201905_n_barometer.html?nn=653844. Vielleicht zeigt die Zunahme an geländegängigen Fahrzeugen aber auch eine neue Perspektive auf: Wenn solche Fahrzeuge nicht auf ausgebaute Straßen angewiesen sind, könnten die Investitionen in den Straßenbau zugunsten der Schiene reduziert werden. Das würde auch die Versiegelung der Böden bremsen.*

21 *Verleihung des BigBrotherAwards 2018 in der Kategorie Politik: https://bigbrotherawards.de/2018/politik-cdu-gruene-landtag-hessen*

22 *Brief an das FIfF: Wir sind Europa – wir sind Nobel? FIfF-Kommunikation 4/2012, S. 4-5*

23 *Nancy Fraser (2017): Vom Regen des progressiven Neoliberalismus in die Traufe des reaktionären Rechtspopulismus. in: Heinrich Geiselberger (Hg.): Die große Regression. Eine internationale Debatte über die geistige Situation der Zeit. Berlin: Suhrkamp*

24 *Rede von Greta Thunberg vor der UN-Klimaschutzkonferenz in Katowice, https://www.youtube.com/watch?v=qvmwt8iJIB4*

25 *Was der syrische Bürgerkrieg mit dem Klimawandel zu tun hat: https://www.sueddeutsche.de/wissen/ausloeser-von-krisen-was-der-syrische-buergerkrieg-mit-dem-klimawandel-zu-tun-hat-1.2377566*

26 *Stefan Hügel (2013): „Politisch Verfolgte genießen Asylrecht". Nachruf auf ein Grundrecht. FIfF-Kommunikation 2/2013, S. 63*

27 *Asylgesetze im Bundestag: Das steckt im Migrationspaket, https://www.spiegel.de/politik/deutschland/geordnete-rueckkehr-gesetz-was-steckt-im-migrationspaket-a-1271323.html*

28 *Pro Asyl, https://www.proasyl.de/news/marathonanhoerung-im-bundestag/*

29 *Verbreitet über Twitter: https://twitter.com/ARD_BaB/status/1136652811045941249. Danach wollte er es offenbar nicht mehr so gemeint haben und bezeichnete er seine Aussage als „ironisch" (https://www.sueddeutsche.de/politik/seehofer-datenaustauschgesetz-1.4479069).*

FIfF e. V. – Pressemitteilung

Das FIfF stützt und bestätigt die Aussagen über Drohneneinsätze der USA, die über die US-Airbase Ramstein in Deutschland koordiniert werden

25. Mai 2019 – *Das Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF) e. V. beschäftigt sich seit mehr als drei Jahrzehnten mit dem Thema Rüstung und Informatik sowie der Militarisierung der Gesellschaft. In diesem Rahmen verfolgen wir auch die globalen Entwicklungen rund um die (informations-)technische Konstruktion, den strategischen Einsatz und die politischen Versprechen rund um militärische Drohneneinsätze, wodurch auch aktuelle und vergangene Kriegshandlungen in unserem Fokus liegen. Dies sind die Kernthemen, die unsere Arbeitsgruppe Rüstung & Informatik (RUIN) kritisch bearbeitet.*

Im kürzlich viral gegangenen Politvideo *Zerstörung der CDU*[1] thematisiert der Youtuber Rezo die Zerstörung des bewohnbaren Planeten durch die Untätigkeit der CDU und teilweise auch der SPD. Zusätzlich geht er auf die deutsche Beteiligung an US-initiierten Kriegseinsätzen ein, sowohl durch direkte Beteiligung durch Aufklärungsmissionen, wie im Syrienkrieg (für den es kein UN-Mandat gibt) als auch durch Bereitstelllung der Kommunikationsinfrastruktur zur Drohnensteuerung (sogenannte Relay-Funktion) in der US-Airbase Ramstein auf deutschem Staatsgebiet, welche die tödlichen Drohneneinsätze überhaupt erst ermöglicht.[2]

Das FIfF unterstützt an dieser Stelle die scharfe Kritik Rezos an der deutschen Regierung, US-geführte Drohnenmorde zu ignorieren. Für weitere Informationen dazu empfehlen wir die Quellen und Belege des Bündnisses Stopp-Ramstein[3], an dem auch das FIfF beteiligt ist. Dort finden sich Belege über ermordete Hochzeitsgesellschaften, Stammesversammlungen oder Krankenhauspersonal – die Zahl der zivilen Opfer, die billigend in Kauf genommen werden, ist erschreckend hoch.

Auch die Tötung von Terror-Anführern wie Osama bin Laden geschieht ohne rechtstaatlichen Prozess, ohne Anhörung, ohne Rechtsbeistand und somit ohne Gerechtigkeit. Dieses Vorgehen ist eines Rechtstaats unwürdig, scharf zu verurteilen und keinesfalls zu unterstützen. Es ist daher erschreckend, dass der damalige verbale Ausrutscher der Bundeskanzlerin, die Tötung ausdrücklich zu begrüßen, heute erneut zustimmend aufgegriffen wird. Dies zeigt anschaulich die Erosion rechtsstaatlicher Prinzipien, nicht nur bei der CDU.

Durch die Enthüllungen von Edward Snowden wissen wir, dass der US-Präsident jeden Dienstag die neuen „Ziele" zum Abschuss freigibt – dafür steht der Name *Terror-Tuesday*.[4] Dabei hat sich die Praxis des *Double Tap* etabliert, wobei nach dem eigentlichen Drohnenschlag gewartet wird, um später noch die dann Helfenden mitzuermorden.[5] Es muss die Frage erlaubt sein, wer hier eigentlich den Terror verbreitet. Angefangen hat diese Vorgehensweise im Übrigen unter dem US-Präsidenten und Friedensnobelpreisträger Barack Obama.

Und auch wenn keine Drohnen eingesetzt werden, sondern Luft- und Bodentruppen, geht es nicht gerechter zu. Die weiteren in Rezos Video angesprochenen Fälle der durch US-Soldaten getöteten Reuters-Reporter, hinzueilenden Helfer und anwesenden Kinder offenbaren zusätzlich ein Kriegsverständnis, was kein moderner Staat praktizieren oder unterstützen sollte. Die Whistleblowerin Chelsea Manning wurde für das *Collateral murder*-Video, das von Rezo als Beleg referenziert wird, zu einer Jahrzehnte langen Gefängnisstrafe verurteilt und auch der

veröffentlichende Wikileaks-Journalist Julian Assange schwebt aktuell in höchster Gefahr, an die USA ausgeliefert zu werden. Dort soll er nach dem umstrittenen *Espionage Act* von 1917 verurteilt werden. Wenn keine Aspekte des Einsatzes verheimlicht werden sollten[6], warum werden dann die Personen mit absurd hohen Freiheitsstrafen bestraft bzw. bedroht, die diesen Einsatz öffentlich machten?

Selbst wenn das Argument einer „Selbstverteidigung der USA" nach den furchtbaren Anschlägen auf das World Trade Center am 11. September 2001 für gültig erachtet würde, so muss doch nach nunmehr 20 Jahren „Krieg gegen den Terror" ein vernichtendes Fazit gezogen werden: In die Steinzeit zurückgebombte Länder, mit bewussten Lügen begründete Kriege, zig Millionen ziviler Opfer, ein dysfunktionaler mittlerer Osten und das überhaupt dadurch erst entstandene Terrorregime „Islamischer Staat"[7] verlangen ein sofortiges Ende dieses „Krieges".

Auch zur Erneuerung der in Deutschland gelagerten US-Atomwaffen hat das FIfF eine klare Position: Wer in dieser Rhetorik des Kalten Kriegs argumentiert und handelt, bekommt letztendlich auch einen neuen Kalten Krieg. Gründungsursache für das FIfF war die Stationierung von computergestützen US-Atomraketen in Deutschland im Jahre 1984, die die Welt damals an den Rand eines Atomkriegs führte. Diese Spirale der Aufrüstung darf nie wieder begonnen werden.

Zusammengefasst sind die von Rezo aufgezeigten Standpunkte grundsätzlich korrekt, gut begründet und in ihrer Dramatik auch erstaunlich verständlich dargestellt.

Anmerkungen

1 *https://www.youtube.com/watch?v=4Y1lZQsyuSQ*
2 *https://daserste.ndr.de/panorama/aktuell/Brandon-Bryant-Ramstein-ist-absolut-zentral,drohnen250.html*
3 *https://www.ramstein-kampagne.eu/category/beitraege_zur_diskussion/*
4 *https://www.zeit.de/politik/deutschland/2013-06/barack-obama-hoffnungstraeger-rede-berlin*
5 *https://www.bbc.com/news/world-us-canada-24557333*
6 *https://www.cdu.de/sites/default/files/media/dokumente/wie-wir-die-sache-sehen.pdf*
7 *https://www.zeit.de/politik/ausland/2015-10/islamischer-staat-tony-blair-irakkrieg-invasion*

Hans-Jörg Kreowski

Ein kurzer Einblick in die Arbeit der Enquête-Kommission Künstliche Intelligenz

Der Bundestag hat vor einem Jahr die Enquête-Kommission Künstliche Intelligenz – Gesellschaftliche Verantwortung und wirtschaftliche, soziale und ökologische Potenziale *eingesetzt. Die Kommission hat den Auftrag, Handlungsempfehlung im Umgang mit Künstlicher Intelligenz (KI) zu formulieren. Ein Teil der Arbeit findet in sechs Projektgruppen (zu Wirtschaft, Staat, Gesundheit, Arbeit/Bildung/Forschung, Mobilität und Medien) statt, von denen drei parallel arbeiten. Die Projektgruppe* KI und Staat *hat mich als „Anhörperson" für die Sitzung am 6. Mai zu einer Diskussion über das Thema* KI und äußere Sicherheit *eingeladen.*

Auf der Webseite des Bundestags heißt es zu den Zielen der Enquête-Kommission:

> *„Der Bundestag greift mit der Enquête-Kommission … eine der zentralen Debatten unserer Zeit auf. Die Enquête-Kommission, die sich zu gleichen Teilen aus Mitgliedern des Deutschen Bundestages und sachverständigen externen Expertinnen und Experten zusammensetzt, soll den zukünftigen Einfluss der Künstlichen Intelligenz (KI) auf unser (Zusammen-) Leben, die deutsche Wirtschaft und die zukünftige Arbeitswelt untersuchen. Erörtert werden sowohl die Chancen als auch die Herausforderungen der KI für Gesellschaft, Staat und Wirtschaft. Zur Diskussion stehen eine Vielzahl technischer, rechtlicher und ethischer Fragen. Zum Auftrag der Enquête-Kommission gehört, … auf Basis ihrer Untersuchungsergebnisse den staatlichen Handlungsbedarf auf nationaler, europäischer und internationaler Ebene zu identifizieren und zu beschreiben, um einerseits die Chancen der KI wirtschaftlich und gesellschaftlich nutzbar zu machen und ihre Risiken zu minimieren."*

Für meinen Vortrag standen 20 Minuten zur Verfügung. Nach mir hatte Rüdiger Bohn aus dem Auswärtigen Amt (Vertreter des Beauftragten der Bundesregierung für Fragen der Abrüstung und Rüstungskontrolle) ebenfalls 20 Minuten Zeit, zu *KI, äußere Sicherheit und Verteidigung* zu sprechen. Danach war noch gut 30 Minuten Zeit für Diskussion. Ich war um eine kritische Bestandsaufnahme sowie um Handlungsempfehlungen und Perspektiven zum Vortragsthema *KI, Militärtechnik und Frieden* gebeten worden. Es folgt mein Fazit, das den kurzen Vortrag weitgehend widerspiegelt.

KI, Militärtechnik und Frieden

Künstliche Intelligenz gilt als Schlüsseltechnologie für die zukünftige Entwicklung von Wirtschaft und Gesellschaft, der sogar teilweise geostrategische Bedeutung zugewiesen wird. Das trifft nicht nur für den zivilen Bereich zu, sondern mindestens in gleicher Weise für den militärischen.

1. These zum Status quo

Die KI-Strategie der Bundesregierung vom November 2018 behandelt detailliert zivile Perspektiven der KI, weist aber sehr wohl auch auf die Forschung zu KI-Anwendungsmöglichkeiten insbesondere zum Schutz der äußeren Sicherheit und für militärische Zwecke sowie auf die Auswirkungen hin, die der künftige Einsatz von KI-basierten Technologien und Systemen auf Streitkräfte haben wird, so dass das ein wichtiges Thema für die Zukunftsent-

wicklung der Bundeswehr sein wird. In einem Interview, das die Redaktion der Bundeswehr mit dem Abteilungsleiter des Fraunhofer-Instituts für Intelligente Analyse- und Informationssysteme, Uwe Beyer, im November 2019 geführt hat, nennt dieser als mögliche Einsatzfelder von KI-Systemen in der Bundeswehr Entscheidungsunterstützungssystemen, intelligenter Datenauswertung in der Aufklärung, autonomen Waffen, Chatbots als Wirkmittel der operativen Kommunikation und selbstoptimierenden Logistiksystemen. Das deckt sich weitgehend mit den KI-Anwendungsbereichen, die in einem im Februar herausgegebenen Strategiepaper des Pentagon als Antwort auf entsprechende Entwicklungen in China und Russland genannt werden. Dort werden allerdings noch als zusätzliche Einsatzfelder automatische Gefahrenerkennung und Risikominimierung aufgeführt. Es scheint also im militärischen Bereich weltumspannend gewisse gemeinsame Vorstellungen zum KI-Einsatz zu geben. Nach meinem Eindruck handelt es sich allerdings weitgehend um Wunschdenken; die Umsetzbarkeit solcher Anwendungen ist noch völlig ungeklärt – mit Ausnahme der autonomen Waffen.

2. These zu letalen autonomen und fast-autonomen Waffen

Nach der *Unmanned Systems Integrated Roadmap* des *Department of Defense* der USA ist mit Milliardenaufwand geplant, einen erheblichen Teil der Bewaffnung auf unbemannte Systeme umzustellen, wobei autonome Systeme einen Schwerpunkt bilden. Man darf wohl davon ausgehen, dass andere Staaten ähnliche Programme verfolgen. Bei bewaffneten Drohnen, die ja schon über ein Jahrzehnt von den USA eingesetzt werden, ist klar, dass zumindest Israel und China gleichwertige Systeme entwickelt haben. Auch in Europa soll eine bewaffnete Drohne entwickelt werden; bis dahin least die Bundeswehr israelische bewaffnungsfähige Drohnen. Diese Drohnen fliegen autonom und suchen autonom Ziele und Zielpersonen, nur der Einsatz von Raketen zur Zerstörung der gefundenen Ziele bzw. Tötung der Zielpersonen wird vorläufig noch von Drohnenpilotinnen und -piloten entschieden. Allerdings sind die automatisch erstellten Informationen über Ziele in einem so hohen Maß suggestiv, dass die Entscheidung über Leben und Tod durch Menschen äußerst eingeschränkt ist. Ein Indiz dafür ist, dass es bei den Einsätzen der Vergangenheit viele zivile Opfer gegeben hat. Das deutet darauf hin, dass auch jetzt schon ohne volle Autonomie die Zielerkennung häufig völkerrechtswidrig erfolgt.

Bei letalen autonomen Waffen gibt es eine recht breite Front in Politik, Wissenschaft und sogar Militär, die für ein Ächtung solcher Waffen eintreten. So plädieren im Rahmen der *United Nations Convention on Conventional Weapons Group of Governmental Experts*, die sich seit einigen Jahren regelmäßig zum Umgang mit letalen autonomen Waffen treffen, 26 (von über 100) Länder für ein Verbot.

Als wesentliche Begründung wird angeführt, dass aus ethischen Erwägungen der Mensch die Kontrolle über Leben und Tod behalten muss und nicht an technische Systeme delegieren darf. Ich selbst halte es aus meiner fachlichen Sicht für praktisch ausgeschlossen, dass sich die Regelungen des Kriegsvölkerrechts (wie beispielsweise der Schutz der Zivilbevölkerung) programmieren lassen. Das ist aber beim Einsatz von autonomen Kriegswaffen erforderlich. Darüber hinaus sehe ich weder technisch noch ethisch-rechtlich große Unterschiede zwischen letalen autonomen Waffen und den weitgehend autonomen. Ganz ähnlich muss man aus meiner Sicht auch der zukünftigen Verwendung von KI-Systemen beim Waffeneinsatz sehen. Wenn beispielsweise eine automatische Gefahrenanalyse einen Angriff irgendeiner Miliz meldet, darf der Gegenangriff nicht auch automatisch ablaufen. Denn die Analyse kann falsch sein.

3. These zu Unzuverlässigkeit und mangelnder Glaubwürdigkeit

Die Fehlerhaftigkeit, Undurchschaubarkeit und mangelnde Zuverlässigkeit – manchmal bis hin zu völliger Unbrauchbarkeit – von computer-gestützten informationstechnischen Systemen ist ein Dauerproblem der Informatik. Die durchaus beachtlichen methodischen Fortschritte der letzten Jahrzehnte haben dennoch nicht Schritt halten können mit den gewachsenen Ansprüchen an Größe und Komplexität der IT-Anwendungen. Bei KI-Systemen und KI-Anwendungen potenzieren sich die Probleme noch, weil die meisten KI-Verfahren sich schwer oder gar nicht durchschauen lassen und ihre Wirkungsweise nur bedingt oder gar nicht vorhersagbar ist. Das gilt insbesondere auch für militärische Anwendungen, weil die oft noch größer, komplexer und anspruchsvoller sind als zivile.

Ein Teil der großen Erfolge der KI in den letzten Jahren (z. B. bei Sprach- und Bildverarbeitung) beruht auf Maschinenlernen und hier insbesondere auf dem sogenannten *Deep Learning*. Dahinter verbergen sich schon lange bekannte Verfahren und Methoden aus der Wahrscheinlichkeitstheorie und Statistik, die jetzt wegen der erreichten Rechengeschwindigkeiten und Datenspeichergrößen greifen. Sie funktionieren allerdings nur, wenn große Zahlen an Musterbeispielen vorliegen, die zum Trainieren der Systeme verwendet werden können. Bei vielen der intendierten militärischen Anwendungen wie Risikominimierung, Gefahrenanalyse, Aufklärung und Waffeneinsatz ist jedoch, soweit ich das sehe, gar nicht geklärt, ob solche für den jeweiligen Zweck geeigneten Datensätze in ausreichend großer Zahl vorhanden sind oder verfügbar gemacht werden können. Neben der „normalen" Fehlerhaftigkeit von IT-Systemen kommt hier also auch das Problem zum Tragen, dass die eingesetzten Methoden für die Problemlösung ungeeignet sein können. Wie lässt sich dann die Glaubwürdigkeit der Berechnungen von militärischen KI-Systemen sicherstellen, wenn diese Vorhersagen zu feindlichen Aktivitäten machen? Kann dann überhaupt noch eine systemunabhängige Kontrolle erfolgen? Wohl kaum. Es ist also höchste Vorsicht geboten.

4. Handlungsempfehlungen

Wegen der mit letalen autonomen Waffen verbundenen ethischen und technischen Probleme sollte Deutschland für eine uneingeschränkte Ächtung solcher Systeme auf internationaler Ebene eintreten und auf nationaler Ebene einen unbedingten Verzicht festschreiben.

Die Abrüstungs- und Rüstungskontrollinitiativen sollten auf fast-autonome Kampfdrohnen und auch auf zukünftige KI-gestützte Kriegswaffen ausgedehnt werden, weil die ganz ähnliche Probleme mit sich bringen wie die letalen autonomen Waffen.

Militärtechnische KI-Forschung in Deutschland sowie Planung und Einsatz von KI in der Bundeswehr sind äußerst intransparent. Da sie aber Risiken bergen und nicht einmal klar ist, ob sie funktionieren, sollte ein Diskurs organisiert werden, der die Entwicklungen unter Beteiligung aller gesellschaftlichen Gruppen und mit einer kritischen wissenschaftlichen Begleitung.

Wegen der geforderten Kürze bleibt diese Zusammenfassung notwendigerweise oberflächlich. Und es ist ziemlich klar, dass ich mit meinem kurzen Vortrag auf die Ergebnisse der Enquête-Kommission nur geringfügigen Einfluss genommen habe. Aber der Besuch im Paul-Löbe-Haus war dennoch eine wertvolle Erfahrung. Mein Eindruck ist, dass die Kommission schon seriös arbeitet und zumindest teilweise um Einsicht bemüht ist, dass aber die Arbeit auch überlagert ist von vorgefassten Positionen und parteipolitischen Aspekten. Bemerkenswert für mich war, dass der Vertreter der Regierung gar nicht so viel anders als ich argumentiert hat. So sei die Regierung beispielsweise auch für das Verbot von autonomen Angriffswaffen, schließt sich jedoch nicht den Staaten an, die ein Verbot fordern, weil dann jedweder Einfluss auf die Verbotsgegner verloren ginge. Naja. Ein Ärgernis im Zusammenhang mit der Enquête-Kommission KI bildet der Umstand, dass ihre Arbeit weitgehend hinter verschlossenen Türen stattfindet und dass die Öffentlichkeit nur völlig unzulänglich einbezogen ist. Die Kommission verpasst die Chance eines breiten und offenen gesellschaftlichen Diskurses. Schade.

FIfF e. V.

FIfF-Konferenz 2019: Künstliche Intelligenz als Wunderland

22. – 24. November 2019 in Bremen

Politik und Wirtschaft scheinen Wunderdinge von der Künstlichen Intelligenz (KI) zu erwarten. Eine Reihe von Fachleuten bestärkt die hochgeschraubten Erwartungen und Hoffnungen durch vollmundige Ankündigungen. Das Wissenschaftsjahr der KI ist ausgerufen. Die Bundesregierung hat eine KI-Strategie auf den Weg gebracht, durch die Deutschland und Europa führend auf dem Gebiet der KI werden sollen – finanziell unterfüttert mit bescheidenen 3 Milliarden Euro. Ihr geht es um den Ausbau der „Wettbewerbsfähigkeit der deutschen Wirtschaft" und um einen „spürbaren gesellschaftlichen Fortschritt". Der Bundestag hat sich vor einem Jahr eine Enquete-Kommission KI mit dem Zusatz „Gesellschaftliche Verantwortung und wirtschaftliche, soziale und ökologische Potenziale" gegeben, um damit „eine der zentralen Debatten unserer Zeit" aufzugreifen. Man kann nur wünschen, dass die Abgeordneten vernünftige Einsichten gewinnen. Auf der Weltbühne ist ein geostrategisches Wettrennen entbrannt, wer bei KI die Nase vorn hat. Die FIfF-Konferenz bietet Gelegenheit, mehr über das Wunderland der KI zu erfahren und sich darüber auszutauschen.

Das Programm nimmt langsam Formen an. Los geht es am Freitagabend im Überseemuseum mit zwei oder drei Vorträgen. Am Samstag und Sonntag wird die Konferenz in der Universität Bremen fortgesetzt mit weiteren Vorträgen, mit parallelen Arbeitsgruppen und der Verleihung des Weizenbaum-Studienpreises. Sie endet am Sonntag mit der FIfF-Mitgliederversammlung. Einige Vorträge stehen bereits fest, auf die man sich schon freuen kann:

- Marit Hansen (Landesbeauftragte für Datenschutz Schleswig-Holstein, Unabhängiges Landeszentrum für Datenschutz): *Die Empfehlungen der Datenethikkommission: Bedeutung für die Informatik*
- Rainer Rehak (Weizenbaum-Institut für die vernetzte Gesellschaft Berlin und FIfF-Vorstand): *Folgenreiche Verführung – Begriffskritik autonomer und intelligenter Systeme*
- Elke Schwarz (Queen Mary University London): *Silicon Valley zieht in den Krieg: Künstliche Intelligenz, autonome Waffen und politisch-moralische Verkümmerung*
- Alexander von Gernler (Vizepräsident der Gesellschaft für Informatik und Leiter der Forschung bei der genua GmbH): *Geschlossene Gesellschaft – Von der Verantwortung der Informatik*

Außerdem werden ein Vertreter von capulcu und Christoph Marischka (Informationsstelle Militarisierung Tübingen) – vielleicht nicht allein – vortragen. Der eine oder andere Vortrag wird noch dazukommen.

Kontakt und weitere Information:
Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e. V., Goetheplatz 4, 28203 Bremen,
fiff@fiff.de;

Kontakt/Anmeldung:
kontakt@fiffkon.de, Pressekontakt: *presse@fiffkon.de*,
Twitter *@fiffkon*, *https://2019.fiffkon.de*.

Über Euer Interesse und Eure Teilnahme würden wir uns freuen.

Um eine bessere Planung zu ermöglichen, bitten wir um (unverbindliche) Anmeldung per E-Mail (siehe *https://2019.fiffkon.de*).

Mit FIfFigen Grüßen

Euer FIfFKon2019-Vorbereitungsteam

FIfF-Konferenz 2018

Brave new World –

Gestaltungsfreiheiten und Machtmuster soziotechnischer Systeme

Teil 2

Editorial zum Schwerpunkt

Viele Produkte, Entwicklungen und Einsatzfelder der Informatik scheinen sich unausweichlich und technisch notwendig so entwickelt zu haben, wie wir sie heute kennen. Seien es die Mechanismen sozialer Netzwerke, der aktuelle Ansatz Künstlicher Intelligenz, das Vorhandensein globaler IT-Monopole, zentralisierte Smart-City-Konzepte oder der wenig regulierte Adress- und Datenhandel. Technische Entwicklungen bauen aufeinander auf, aber finden natürlich nicht im luftleeren Raum statt. Es gibt immer verschiedene Wege, ein Problem anzugehen und entsprechend Ressourcen für dessen Lösung aufzuwenden.

Oftmals liegen den tatsächlichen Entwicklungen gerade keine primär technischen Überlegungen zu Grunde, sondern ökonomische oder politische Motive. Folglich ist es erhellend, Informatik- und Technikgeschichte auch unter diesen Aspekten zu betreiben. So können Entscheidungsalternativen oder Weggabelungen herausgestellt werden, um die dahinterliegenden Machtinteressen, aber auch die sachlichen wie sozialen Dynamiken und Zwänge freizulegen. Dieses Wissen ermöglicht es dann, heutige technische Entwicklungen und Weichenstellungen besser zu verstehen.

Doch wir wollen auch aktiv an aktuellen und zukünftigen tiefgreifenden Veränderungen mitwirken, denn die Informatik ist immer auch Gestaltungsdisziplin – weit über die reine Technik hinaus. Wir wollen also mithelfen, die stetige Digitalisierung und Vernetzung der Gesellschaft so mitzuprägen, dass die Freiheit des Individuums und das Wohl der Gesellschaft im Vordergrund jeglicher Technikentwicklung und ihres Einsatzes stehen – sowohl in unseren Endgeräten und Anwendungen als auch in unserer digitalen Infrastruktur.

Wir wollen Sichtweisen und konkrete Wege erarbeiten, auf welche Weise nicht-technische Werte wie demokratische Teilhabe, Freiheit und Selbstbestimmung, Pluralismus von Lebensentwürfen und Nachvollziehbarkeit von Entscheidungen genauso in technischen Systemen und den politischen Entscheidungen darüber Eingang finden, wie die Verhinderung verdeckter Machtzentren, die Bekämpfung von Diskriminierung und struktureller Benachteiligung, Privatisierung staatlicher Kernaufgaben. Wir wollen keine smarten Privatstädte mit herrlichem Kundenerlebnis, sondern lebendig-diverse Städte mit emanzipierten BürgerInnen. Wir wollen keine zentralisierten Infrastrukturen, die von globalen, intransparenten Konzernen betrieben werden, sondern dezentralisierte und selbstverwaltete Systeme. Wir wollen unsere Kommunikationsmittel nicht von Geheimdiensten und Militär durchdrungen wissen, sondern integre und vertrauliche Systeme mit Respekt sowie Vertrauen in Menschen und ihre Grundrechte. Wir wollen diese Werte konkret realisiert sehen.

Die Informatik erlaubt all dies in ihren Systemen. Wir müssen die Freiheitsgrade der Technik ausnutzen, aber vor allem müssen wir den politischen Willen dafür aufbringen. Wir wollen tatsächlich mutig sein und mit den Vorträgen dieser Konferenz dazu beitragen, eine neue, bessere Welt für alle Menschen zu erdenken um sie dann zu bauen.

Dieser Schwerpunkt der FIfF-Kommunikation enthält den zweiten Teil der Beiträge zu der Konferenz. Ganz herzlichen Dank an alle Helferinnen und Helfer, die die Beiträge zusammengestellt haben und ohne die diese Ausgabe in der vorliegenden Form nicht möglich gewesen wäre. Die Transkripte und Zusammenfassungen wurden mit größter Sorgfalt erstellt und aus Zeitgründen i. d. R. nicht autorisiert – alle verbliebenen Fehler gehen damit zu Lasten der Redaktion.

Wegen des Umfangs des Materials teilen wir diesen Schwerpunkt auf zwei Hefte auf – hier folgen die Beiträge, die in Ausgabe 1/2019 keinen Platz mehr gefunden haben, genauso wie die Beiträge der Preisträger des Weizenbaum-Studienpreises.

Den Anfang macht *Florian Schumacher*: *Cyber-Sicherheit in der Digitalisierung – eine Herausforderung für Staat, Wirtschaft und Gesellschaft* ist der Titel seines Beitrags. Cyber-Sicherheit stellt eine Vorbedingung für das Gelingen der Digitalisierung dar. Dass die Gewährleistung von Sicherheit im digitalen Raum eine zentrale Herausforderung darstellt, zeigt der Bericht zur Lage der IT-Sicherheit in Deutschland des BSI in jedem Jahr eindrücklich.

Das BSI arbeitet mit verschiedenen Akteuren aus Staat, Wirtschaft und Gesellschaft gemeinsam daran, den Risiken wirksame und umsetzbare Sicherheitsmaßnahmen entgegenzusetzen und die Widerstandsfähigkeit Deutschlands gegen Cyber-Gefahren zu erhöhen. Florian Schumacher, Referent für Cyber-Sicherheit für die Gesellschaft, geht in seinem Beitrag u. a. auf die aktuelle Cyber-Sicherheitslage in Deutschland ein, er stellt die Rolle des

BSI als die nationale Cyber-Sicherheitsbehörde vor und präsentiert die Aktivitäten als gesellschaftlicher Gestalter von Cyber-Sicherheit.

Der nächste Beitrag von *Rainer Mühlhoff* beschäftigt sich mit *Digitale Entmündigung und „UserExperience Design". Über Nudging, Tracking und Infantilisierung im Netz*. Die letzten 10 Jahre haben nicht nur den Durchbruch von Smartphones, Cloud-Diensten und Künstlicher Intelligenz gebracht. Zeitgleich ist im Netz eine universelle Infrastruktur zum Sammeln von Bewegungs- und Nutzungsdaten entstanden, der zu entkommen längst auch für versierte User schwierig geworden ist.

Der Beitrag beschäftigt sich mit den gesellschaftlichen Folgen und sozialen Dimensionen dieser Datenaggregation. Eine zentrale Rolle spielt dabei – vielleicht unerwartet – ein genauerer Blick auf die Praktiken des User Experience Designs. Mühlhoff diskutiert verschiedene Tricks, wie kommerzielle Akteure ihre Nutzer dazu bringen, oft unwissentlich ihre Daten zur Verfügung zustellen. Er diskutiert, wie diese Daten dazu verwendet werden, Nutzerverhalten vorherzusagen und zu beeinflussen. Unter dem Schlagwort „digitale Entmündigung" argumentiert er, dass es in der aktuellen Netzkultur eine systematische Tendenz dazu gibt, die User ihrer Fähigkeit zum verständigen und selbstbestimmten Umgang mit digitalen Diensten zu berauben. Mit Blick auf die Datenschutzdebatte stellt er schließlich das politische Problem massenweiser, prinzipiell auch anonymisierter Datensammlung scharf und er geht auf die Dimension sozialer Ungleichheit und automatisierter Selektion ein, die durch prädiktive Verhaltensanalytik und Profilbildung möglich wird.

Die Grenzen der Automation durch Künstliche Intelligenz: *Wie wissen wir, was automatisiert werden kann und was nicht?* war der Vortrag von *Hendrik Heuer* und *Karen Ullrich* übeschrieben. Leider lag uns zu diesem Beitrag keine Aufzeichnung vor, weswegen wir ihn kurz zusammenfassen.

Während in Statistikkursen ausdrücklich davor gewarnt wird, eine Regressionsanalyse für Bereiche einzusetzen, die außerhalb des Messbereichs liegen, werden die Limitationen von Machine Learning-System selten problematisiert.

Insbesondere in populärwissenschaftlichen Darstellungen und außerakademischen Anwendungen fehlt eine Sensibilität für die Grenzen der Systeme und mögliche Verzerrungen, die durch Daten und Modellierungsannahmen entstehen können. An konkreten Beispielen werden die Probleme der Annahme aufgezeigt, dass Machine Learning-Systeme universell einsetzbar sind.

In einer *Podiumsdiskussion* zum Thema künstliche Intelligenz diskutieren *Aljoscha Burchardt*, *Constanze Kurz* und *Karen Ullrich* über theoretische Grenzen, praktische Möglichkeiten und den politische Diskurs um den KI-Einsatz. Es wird auch um Machtfragen gehen und wer die nötige Daten für ihren Einsatz hat. Wem nützt KI überhaupt und was stellen die Firmen und Staaten damit an? Sollten wir uns primär technisch mit KI beschäftigen oder eher mit denen, die sie für ihre Zwecke nutzen? Zuletzt wird es auch um die Eckpunkte der KI-Strategie der Bundesregierung und um die KI-Enquête des Bundestages gehen? Worüber wird dort gesprochen, worüber nicht? Worüber sollte dort gesprochen werden? Drei ausgewiesene Expertinnen durchdenken diese und andere Fragen gemeinsam mit dem Publikum.

Kirsten Bock und Malte Engeler befassen sich mit der DSGVO: *Eine kommentierte Reise durch die (Un)Tiefen des juristischen Feuilletons – Launige Bilanz nach vier Monaten Geltung.* Vom Foto-Verbot zum Ende strukturierter Visitenkartensammlungen. Vom großen Blogsterben zu Zahnärzten und ihren Datenschutz-Tonbandansagen. Von überforderten Aufsichtsbehörden zu jubelnden Silicon-Valley-Riesen:

Die DSGVO hat all den bekannten Kontroversen des Datenschutzrechts neuen Diskussionsstoff gegeben. Die Twitter-Szene hat die großen, kleinen (und vermeintlichen) Aufreger dankend aufgegriffen. Kirsten Bock und Malte Engeler begeben sich anhand ausgewählter Tweets auf eine kommentierte Twitter-Reise durch die Untiefen des DSGVO-Wahnsinns.

Der letzte Beitrag stammt von *Katika Kühnreich*: *Kybernetik und Kontrolle – Von der autoritären Nutzung von Daten in China und anderswo*. In den letzten Monaten kam die Berichterstattung über die Einführung von Digitalen Gesellschaftlichen Bewertungssystemen (Social Credit Systems) in China in Fahrt, leider auch mit mancher Fehlberichterstattung.

Die Politikwissenschaftlerin und Sinologin Katika Kühnreich gibt in ihrem Vortrag eine Übersicht über existierende Systeme und ihre Funktionen. Doch sie bleibt nicht in China stehen, sondern wirft die Frage auf, wie stark die Tendenz zu Überwachung und autoritären Steuerung von Gesellschaften auch in westlichen Ländern existiert. Bei der Erörterung von sozialen und politischen Auswirkungen wird ein Schwerpunkt auf die Rolle der Kybernetik gesetzt.

Cyber-Sicherheit in der Digitalisierung – eine Herausforderung für Staat, Wirtschaft und Gesellschaft

Verschriftlichung des Vortrags von Florian Schumacher

Florian Schumacher sprach zum Thema Cybersicherheit und ging dabei auf die drei Felder Staat, Wirtschaft *und* Gesellschaft *ein. Sein Vortrag umfasste zuerst die Gefährdungslage und den aktuellen Lagebericht und im Anschluss das Bundesamt für die Sicherheit in der Informationstechnik (BSI) und zwei konkreten inhaltlichen Aufgaben: Schutz von kritischen Infrastrukturen und Cybersicherheit für die Gesellschaft und Dialog. Er selbst arbeitet im Bereich* Cybersicherheit für die Gesellschaft *und kümmert sich um das Thema* Gesellschaftlicher Dialog.

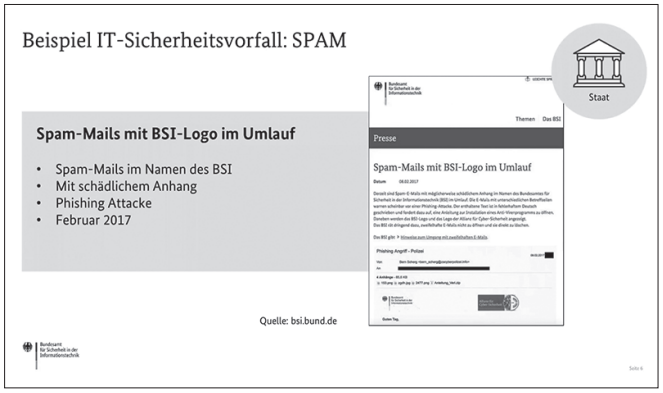
Florian Schumacher beginnt mit der Frage, warum es wichtig ist, sich mit dem Thema Cybersicherheit zu beschäftigen. Er verweist auf Rainer Rehak, der im Rahmen der FIfFkon gesagt hat, Digitalisierung sei kein Thema, das uns jetzt erst seit kurzem beschäftige, sondern sei schon ein lang laufender Prozess. Florian Schumacher weist jedoch darauf hin, dass gerade die Digitalisierungsentwicklung in den letzten Jahren, verkürzt dargestellt durch die drei Begriffe der Vernetzung, der Komplexität und der Allgegenwärtigkeit von IT, es notwendig macht, sich mit dem Thema Cybersicherheit zu beschäftigen. Cybersicherheit stellt eine Voraussetzung für das Gelingen der Digitalisierung dar. Da die Digitalisierung all unseren (sensiblen) Lebensbereiche durchdringt, sind wir abhängig von der Funktionsfähigkeit und Sicherheit der IT. Es betrifft uns individuell in unserer Privatheit, in der Sicherheit unserer Daten, aber auch unsere öffentliche Sicherheit.

Cyberangriffe und Cyberkriminalität sind sehr lukrativ, da man damit sehr viel mehr Geld verdienen kann als beispielsweise mit Drogenkriminalität. Florian Schumacher verweist Interessierte explizit auf den BKA-Lagebericht zu Cybercrime. Außerdem sind Cyberangriffe sehr gezielt und oft lange Zeit unbemerkt vom Opfer, wie vergangene APT- (*Advanced Persistent Threat*-) Angriffe zeigen. Und Cyberangriffe verursachen einen großen volkswirtschaftlichen Schaden von durchschnittlich 55 Milliarden Euro im Jahr. Die verwendeten Schadprogramme zeichnen sich durch eine sehr große Varianz und Schnelllebigkeit aus. Begünstigt werden Cyberangriffe durch ein bestehendes Qualitätsproblem der Software, was die Zahl der bestehenden Sicherheitslücken in den zehn meistgenutzten Softwareprodukten zeigt.

Aktuelle Beispiele für Sicherheitsvorfälle

Florian Schumacher nennt nun einige aktuelle Beispiele von Cybersicherheits- oder IT-Sicherheitsvorfällen und beleuchtet einige Phänomene.

Spam



Er beginnt mit dem Thema *Spam*, vor dem auch das BSI nicht gefeit ist. Es gibt Akteure, die sich Vertrauenswürdigkeit zu Eigen machen und dann Logos des BSI oder auch anderer Unternehmen und Institutionen nutzen, um damit kriminell vorzugehen. Beim Thema Spam gibt es eine Verknüpfung von verschiedenen Phänomenen. Es werden beispielsweise Botnetze genutzt, um Spam zu versenden und Spam wird als konkrete Dienstleistung im Darknet angeboten. Um an die Empfänger-E-Mail-Adressen und -Daten zu kommen, werden Datenabflüsse großer Dienstleister oder Kontaktdaten aus E-Mail-Clients von infizierten Systemen genutzt. Teilweise findet auch die Recherche nach konkreten Kontaktdaten statt.

Advanced Persistent Threat (APT)

Ein Beispiel für einen *APT-Angriff* stellt der Regierungshack dar. Es gab einen Hack der Lernplattform ILIAS (Integriertes Lern-, Informations- und Arbeitskooperations-System) der BAKöV (Bundesakademie für öffentliche Verwaltung im Bundesministerium des Innern, für Bau und Heimat), die an den IVBB (Informationsverbund Berlin-Bonn), also das Behördennetz angeschlossen ist. Dort wurde ein Trojaner eingeschleust, und darüber konnten dann Dokumente beim Auswärtigen Amt ausgeschleust werden. Insgesamt sind die Auswirkungen aufgrund guter bestehender Sicherheitsmechanismen gering. Außerdem war die Beobachtung der Tätergruppierung möglich.

Im allgemeinen stellt Florian Schumacher im Bezug auf APT-Angriffe einen Zuwachs an Installer- oder Update-Hijacking in der initialen Phase fest. Das heißt, es findet eine Schadcodeinfizierung auf Webseiten oder Updateservern von Softwareherstellern statt. Dort werden dann Schadprogramme eingeschleust, die dann vom Nutzer unbewusst heruntergeladen werden. Das Ziel hinter APT-Angrfiffen ist Spionage oder auch Sabotage.

Distributed Denial of Service (DDoS)

Ein weiteres Phänomen stellen sogenannte DDoS-Angriffe dar. Dabei wird versucht, wie am Beispiel der RWE AG, durch eine Vielzahl von Anfragen ein System in die Knie zu zwingen. Bei diesem Phänomen lässt sich eine steigende Tendenz und eine große Bandbreite beobachten. Aufgrund größerer verfügbarer Bandbreite werden Angriffe auf Systeme mit beispielsweise 1 GBit/s durchgeführt. Im Jahr 2018 wurde vom BSI auch eine Rekordbandbreite bei solchen Angriffen festgestellt. Es gab im Frühjahr einen Angriff mit 1,7 TBit/s. Die Motivation der Angreifer in solchen Fällen sind erneut Sabotage, Vandalismus, Manipulation von Systemen oder die einfache Störung.

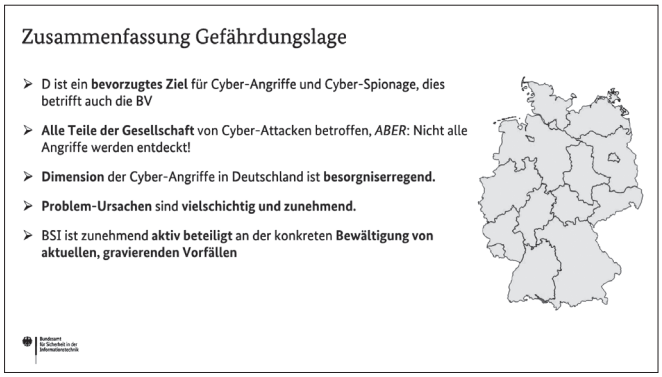
Ransomware

Vom Thema *Ransomware* war im letzten Jahr beispielsweise die Bahn betroffen. Es werden dabei unternehmensinterne Dateien abgegriffen und verschlüsselt und die Angreifer verlangen von den Opfern Geld, um die Dateien wieder zu entschlüsseln. Da einige Opfer kein Backup hatten, gab es manche, die darauf hereingefallen sind und dieses Geld gezahlt haben. Trotzdem haben sie vielleicht am Ende gar keinen Schlüssel zugesendet bekommen. Das BSI hat generell davon abgeraten, solche Lösegeldzahlungen zu leisten. Generell sind Ransomware-Angriffe meist keine gezielten Angriffe, sondern Massenangriffe, und sehr viele Unternehmen waren davon auch schon betroffen. Eine Umfrage der Allianz für Cybersicherheit, die vom BSI betrieben wird, zeigt, dass 22,5 % der befragten Wirtschaftsunternehmen bereits im Jahr 2017 einen Ransomware-Vorfall hatten. Ein Trend, den das BSI in diesem Fall beobachtet, ist, dass es auch immer mehr zu „Ransomware as a service" geht. Das heißt, dass auch weniger technik-bewanderte Nutzer Ransomware-Angriffe mieten können und nach dem Baukastenprinzip den Angriff zielgenau auswählen können. Das läuft interessanterweise manchmal in einem Partnermodell ab bei dem der Dienstleister als Bezahlung einen Teil des Lösegeldes bekommt.

Identitätsdiebstahl

Als letztes Phänomen werden *Identitätsdiebstähle* vorgestellt. Dabei ist der *Yahoo-Hack* am bekanntesten. Er stellt den größten öffentlich bekannten Angriff dar, von dem drei Milliarden Nutzerkonten betroffen waren. Sehr bedauerlich war dabei, dass der Angriff aufgrund der intransparenten Vorgehensweise erst mit großem Zeitabstand bekannt wurde. Das BSI hat in dem Fall eine Kooperationsbereitschaft von Yahoo gegenüber den deutschen Behörden erlebt. In Deutschland selbst sind von solchen Angriffen natürlich die Organisationen betroffen, die sensible Daten haben, wie beispielsweise Banken, Online-Bezahlsysteme

oder auch Online-Händler. In diesen speziellen Fällen machen sich die Angreifer gerade die Vetrauenswürdigkeit der Systeme zunutze. Beispielsweise kommt seit Ende 2017 bei Phishing-Webseiten https zum Einsatz, um dem Nutzer eine größere Vertrauenswürdigkeit der Seite zu vermitteln. Daneben versucht man die Leute zu erreichen, indem man medienpräsente Themen wie DSGVO oder Blockchain auf solchen Fake-Seiten setzt, so dass der Laie ein Interesse für dieses Thema hat und dann vorschnell darauf hereinfällt.



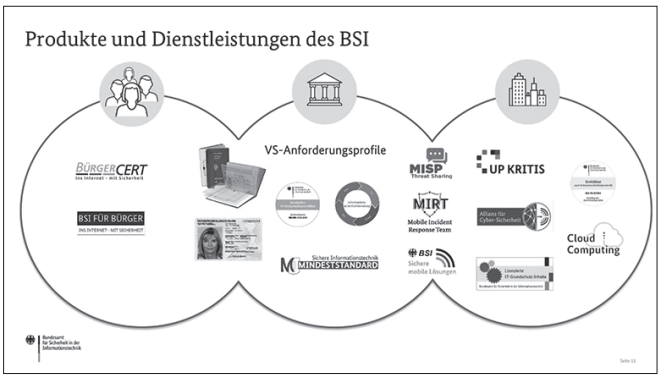
Diese verschiedenen dargestellten Phänomene sollen zeigen, dass von Cyberangriffen und Cyberattacken verschiedene Teile der Gesellschaft betroffen sind, also sowohl staatliche Akteure, wie beispielsweise beim Regierungshack, als auch Wirtschaftsakteure, wie beispielsweise bei RWE, oder natürlich auch kritische Infrastrukturen, wo Industrieanlagen angegriffen werden, ebenso wie individuelle Nutzer. Das gilt auch für Ransomware- oder Identitätsdiebstahl-Angriffe. Generell lassen sich aus Sicht des BSI viele Angriffe durch einfache geeignete Basismaßnahmen in den Kategorien Prävention, Detektion und Reaktion verhindern, oder zumindest in den Auswirkungen minimieren.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI)

Die Übersicht dieser verschiedenen Gefährdungen und Risiken, die es in der digitalen Welt gibt, zeigt, dass es eine Stelle braucht, die sich mit dem Thema beschäftigt und Kompetenzen besitzt, um mit diesen Risiken umzugehen. Das BSI fungiert als diese nationale Cybersicherheitsbehörde und hat dort einen Gestaltungsanspruch in den drei Themenfeldern: präventive Maßnahmen umzusetzen, Detektionsmechanismen zu entwickeln und dann auch reaktionsfähig zu sein. Es versteht sich mit einem ganzheitlichen und kooperativen Ansatz als Dienstleister für die drei Zielgruppen Staat, Wirtschaft und Gesellschaft. Das BSI ist die einzige Behörde mit einem klaren gesetzlichen Auftrag zur Cyberabwehr.

Entwicklung und Aufgaben

Florian Schumacher beschreibt das BSI mit den drei Schlagworten Veränderung, Attraktivität und Vernetzung. Das BSI wurde 1991 gegründet und war ursprünglich nur zuständig für die Absicherung der Regierungskommunikation. Grundaufgaben waren die Verschlüsselung und die Sicherung vertraulicher Regierungskommunikation. Über die Jahre hat sich das verändert und es wurden Informationen und Sensibilisierungsangebote für Bürgerinnen und Bürger bereit gestellt. Hinzu kamen der Schutz von kritischen Infrastrukturen und Aufbau von Austauschformaten für Wirtschaftsunternehmen, Austausch von Erfahrungen und Best Practices etc. In den letzten Jahren ist das BSI stark gewachsen. 2015 hatte das BSI knapp über 600 Mitarbeiter, aktuell sind es ca. 940 und es wird einen weiteren Wachstumstrend geben. Das ist auch ein Indiz dafür, dass das Thema Cybersicherheit stark an Relevanz gewonnen hat und und in der öffentlichen Wahrnehmung präsent ist. Das BSI gehört laut Umfragen zu den Top-Arbeitgebern, das gilt auch im Vergleich zu anderen Behörden. Es verfügt über einen im Vergleich zur Branche überdurchschnittlich hohen Frauenanteil. Das BSI ist eine technische Behörde mit 80 % MINT-Hintergrund. Bei Vernetzung geht es nicht nur um die nationale Vernetzung. Das BSI möchte auch in der Fläche präsenter sein und hat dazu ein Verbindungswesen mit Schwerpunktregionen aufgebaut. Aber auch international ist es sehr anerkannt. Es vertritt die Bundesrepublik in vielen internationalen Gremien der Organisationen, in denen die Bundesrepublik vertreten ist, beispielsweise bei der NATO als verantwortlicher Stelle für das Thema Cybersicherheit und Cyberabwehr oder bei ENISA (European Union Agency for Network and Information Security) als Mitglied im Management-Board. ENISA ist die europäische Organisation, die sich mit dem Thema Cybersicherheit beschäftigt.



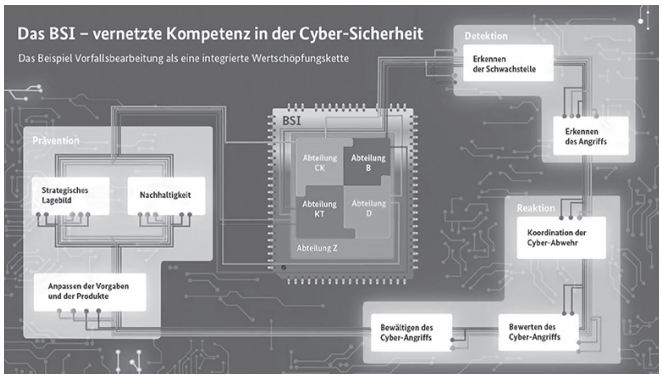
Zielgruppen

Für die drei genannten Zielgruppen, Staat, Wirtschaft und Gesellschaft, gibt es ein Produktportfolio und eine Produktübersicht, wovon Florian Schumacher einige Produkte vorstellt, um einen Gesamtüberblick darüber zu geben, was das BSI macht. Angefangen bei der Gesellschaft sind die Angebote zu nennen, die den Bürger direkt adressieren. Es gibt das BürgerCERT (Computer Emergency Response Team), welches Warnmeldungen über aktuelle Sicherheitsvorfälle herausgibt, auf die Bürger und Bürgerinnen achten müssen, oder Informationen zu Updates bereitstellt. Außerdem existiert *BSI für Bürger* mit verschiedenen Informationsmaterialien und konkreten Checklisten und Broschüren, Onlineauftritten, einer Hotline und einem Servicecenter, bei dem man sich melden kann, wenn es Probleme gibt.

Dann gibt es den Übergang zum Bereich Staat. Das BSI ist bei der Entwicklung von Anforderungen zur Sicherheit elektronischer Identitäten dabei oder entwickelt diese maßgeblich. Sei es beim neuen Personalausweis als auch beim Reisepass. Daneben gibt es dann Angebote, die sich direkt an den Staat richten. Wie bereits gesagt: Das BSI kommt aus dem Bereich der Sicherung der Regierungskommunikation. Da ist das Thema VS-Anforderungsprofile zu nennen. Also wie sichere ich Verschlusssachen?

Was ist dort bei der elektronischen Bearbeitung zu beachten? Dann aber auch das Thema ISMS (Informationssicherheits-Managementsystem). Wie baue ich ein ISMS für meine Behörde auf? Dort gibt es Kollegen, die konkret beraten. Als auch das Thema Mindeststandards. Dort gibt es einen Bereich im BSI, der konktret auch Mindeststandards für bestimmte Themen der Bundesverwaltung entwickelt.

Wenn wir jetzt hinübergehen zum Bereich der Wirtschaft: Dort gibt es auch Themen, die mehr die Schnittstellen betreffen. Da gibt es Plattformen zum Informationsaustausch, wie eine Plattform zum Austausch über Gefährdungsindikatoren bei Malware, die Malware-Informationsharing-Platform. Dann gibt es MIRT-Teams: *Mobile Incident Response Teams*, die sich bei Cybersicherheitsvorfällen an staatliche Stellen, aber auch an Betreiber kritischer Infrastrukturen richten und dann konkret helfen; im Einzelfall flexibel zusammengesetzt werden nach den Experten, dies es für diesen Vorfall braucht, um dann vor Ort zu helfen. Als dritter Punkt: sichere mobile Lösungen, das heißt Lösungen, auf denen man auch eingestufte Informationen bearbeiten kann, sei es ein Smartphone oder ein Tablet, wo es auch eine konkrete Lösung gibt. In dem Feld Wirtschaft gibt es auch unterschiedliche Angebote, die das BSI vorhält. Da werde ich dann gleich noch einmal konkreter zu sprechen kommen zu dem Thema *UP-KRITIS*, einer Plattform der öffentlich-privaten Kooperation von KRITIS-Unternehmen, Verbänden, die mit KRITIS-Unternehmen zu tun haben, und den zuständigen staatlichen Stellen – das sind ja auch ganz unterschiedliche Stellen und Aufsichtsbehörden – um gemeinsam an einem höheren Sicherheitsniveau für kritische Infrastrukturen zu arbeiten.



Dann die Allianz für Cybersicherheit, die als Netzwerk fungiert, als Plattform, wo es zum Erfahrungsaustausch kommen kann von Wirtschaftsunternehmen, mit inzwischen ca. 3000 Mitgliedern. Und das soll auch ein bisschen als Multiplikator dienen, als Netzwerk für das Netzwerk: Das heisst, einzelne Akteure können dort Vorträge halten, können dort Best Practices vorstellen für andere Netzwerkmitglieder. Darüber hinaus gibt es den IT-Grundschutz, der sicherlich auch manchem bekannt ist. Das heisst, ein Instrument, in dem IT-Sicherheitsmaßnahmen aufgeschrieben sind, als systematischer Katalog. Dort ist es möglich für Unternehmen oder auch andere Akteure, sich diesen Katalog anzusehen und dort zu identifizieren: Welche Sicherheitsmaßnahmen brauche ich speziell in meinem Kontext und wie kann ich sie umsetzen?

Für das Thema Cloud-Computing hat das BSI ebenfalls einen Anforderungskatalog entwickelt, der sich an Cloud-Anbieter richtet. Dies ist ein Katalog von Mindestanforderungen, die es zu erfüllen gilt. Und nach diesem Katalog kann sich dann das Unternehmen testieren lassen von einem Wirtschaftsprüfungsunternehmen.

Organisation

Wie arbeitet das BSI konkret? Das möchte ich an einem Beispiel der Vorfallsbearbeitung darstellen. Das BSI besteht aus fünf Abteilungen:

- der Abteilung CK, die sich um die operative Abwehr kümmert, aber auch um KRITIS,
- der Abteilung B, in der ich arbeite, die sich um das Feld Beratung für Staat, Wirtschaft und Gesellschaft kümmert,
- der Abteilung D, die sich mit Mindeststandards und Zertifizierung auseinandersetzt,
- die Abteilung KT, das sind die Kryptographen,
- daneben die Abteilung Z, die sich mit Organisation und Personal beschäftigt.

Wie läuft das ab? Holzschnittartig beschrieben im Bereich der Vorfallsbearbeitung: Bei der Detektion würde beispielsweise die Abteilung CK überhaupt erst einmal über das Lagezentrum feststellen, dass es zu einem Angriff gekommen ist, das heißt die Erkennung von Schwachstellen und Angriffsmethoden. Dann im Bereich der Reaktion und Koordination über das nationale Cyberabwehrzentrum, welches auch dort angesiedelt ist: Bewerten des Angriffs, vielleicht auch Bewerten, was dieser Angriff für Auswirkungen für Unternehmen hat. Was hat er für Auswirkungen für die Bundesverwaltung? Müssen wir dort gewisse Anforderungen erhöhen? Gibt es vielleicht auch Effekte, die sich dann wieder auf die Prävention auswirken müssen? Müssen irgendwelche kryptographischen Verfahren angepasst werden? So fügt sich das dann zusammen, wo jede Abteilung die eigenen Kompetenzen einbringt, allerdings dann auch das nach außen gegenüber ihren Stakeholdern darstellt.

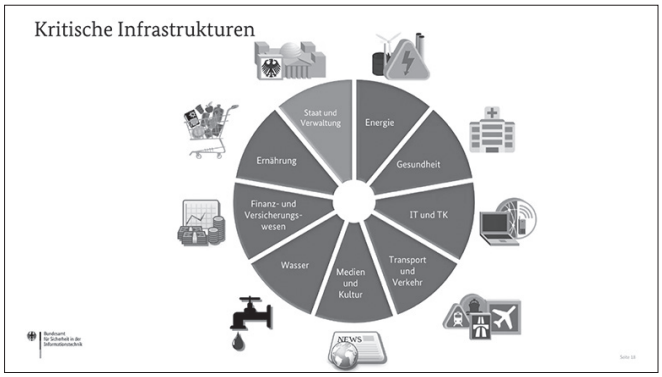
Tätigkeitsfelder des BSI

Um zum konkreten Beispiel zu kommen, zu zwei Feldern in denen das BSI aktiv ist: Ich möchte einmal das Feld KRITIS vorstellen, *Kritische Infrastrukturen* – auch auf konkreten Wunsch der Organisatoren – um zu zeigen, was das BSI macht in diesem Feld, und dann komme ich gleich noch zum Themenfeld *Gesellschaftlicher Dialog*.

Kritische Infrastrukturen (KRITIS)

Kritische Infrastrukturen sind essenziell wichtig für unser tägliches Leben; ihre Betreiber sind essenziell wichtige Dienstleister, sonst hätten wir hier kein Licht, könnten nichts essen, etc. Das Feld wurde in neun Sektoren unterteilt. Wenn wir uns dies ansehen und an unser tägliches Leben denken, stellen wir fest, diese verschiedenen Sektoren sind stark von Informations- und Kom-

munikationstechnologie (IKT) durchdrungen und können auch gar nicht ihre Dienstleistung erbringen, ohne dass sie eine funktionierende Unterstützung durch IKT haben. Seit 2015 gibt es mit dem IT-Sicherheitsgesetz eine gesetzliche Grundlage zum Schutz von kritischen Infrastrukturen und das BSI setzt dieses IT-Sicherheitsgesetz um, das heisst, beim BSI können sich Unternehmen aus dem Bereich der kritischen Infrastrukturen, die unter diese Definition fallen und aus diesen Bereichen kommen, registrieren. Sie werden dort in ein Meldewesen eingebunden, das heisst, wenn sie einen IT-Sicherheitsvorfall haben, wird dieser ans BSI gemeldet, und gleichzeitig überprüft das BSI die Umsetzung von Sicherheitsmaßnahmen dann durch Audits.



Für die verschiedenen Zielgruppen des BSI haben wir eine Dienstleistungspyramide entwickelt, die so zu verstehen ist, dass das, was ganz unten ist, das Thema Information, den geringsten Bereitstellungsaufwand hat. Das steigt dann immer weiter nach oben. Natürlich wäre der höchste Aufwand, wenn das BSI oder Kollegen des BSI konkret technische Schutzmaßnahmen übernehmen. Das ist im Bereich KRITIS nicht vorgesehen. Bei anderen Organisationen oder beim Staat sieht das dann anders aus. Das BSI hat ein ziemlich breites Angebot, wenn man diese Pyramide betrachtet für den Bereich der kritischen Infrastrukturen. Angefangen unten natürlich beim Thema Information. Den IT-Grundschutz hatte ich schon genannt, Es gibt aber auch technische Richtlinien, nach denen man sich richten kann. Es gibt Cybersicherheits-Empfehlungen. Das Thema Abstrahlprüfung könnte auch interessant sein. Es gibt allgemeine Lageberichte und es gibt spezielle Lagenerichte, auch für kritische Infrastrukturen.

Das BSI ist aber auch tätig für kritische Infrastrukturen im Bereich der Aus- und Fortbildung, das heisst, wir gehen auf Veranstaltungen von Verbänden etc., wo für Themen der Cybersicherheit sensibilisiert wird.

Und dann in der Mitte eins der wichtigsten Felder: Kooperation. Weil gerade bei KRITIS, aber auch generell, das BSI einen kooperativen Ansatz hat. Es sind keine Alleingänge möglich. Das betrifft sowohl die Unternehmen als auch das BSI selbst. Das heißt, es gibt UP-KRITIS als Plattform, wo 600 verschiedene Akteure (Unternehmen, Verbände, staatliche Akteure) organisiert sind mit Branchen und Themenarbeitskreisen. Die Branchen richten sich nach den verschiedenen Themenbereichen, die ich dargestellt habe. Dann gibt es die Allianz für Cybersicherheit, das heisst, Unternehmen, die nicht unter die KRITIS-Definition fallen, wie beispielsweise Institutionen mit besonderem staatlichen Interesse, können sich auch in dieser Allianz organisieren. Wie ich schon sagte, dies ist eine große Gruppe von Akteueren. Dort gibt es wiederum Themenarbeitsgruppen und andere Angebote, wo man sich auch austauschen oder Informationen einholen kann. Sie veranstalten Cybersicherheitstage, die um ein spezielles Thema gehen. Das heißt, wenn ich Input zu einem speziellen Thema brauche, kann ich dorthin gehen. Das Thema nationales Verbindungswesen habe ich eben schon erläutert.

Dann gibt es aber auch konkrete Beratungsdienstleistungen, die durch das IT-Sicherheitsgesetz reguliert sind. Beispielweise meldet ein Unternehmen einen Vorfall und kann dann auf diese Beratungsdienstleistungen zurückgreifen. Aber es gibt auch vom BSI zertifizierte Dienstleister, die in einem solchen Fall konkrete Hilfe vor Ort leisten können.

Technische Unterstützung und Dienstleistungen: Die Abkürzung B3S bedeutet, es gibt branchenspezifische Mindeststandards, das heisst, die Unternehmen müssen sich nach dem Stand der Technik richten und können dann für sich als Branche einen Stand der Technik definieren. Dieser wird dann vom BSI überprüft. Es gibt schon verschiedene Bereiche, die das für sich getan haben. Wer heute auf die BSI-Webseite klickt, wird sehen, es wurde kürzlich erst aus dem Bereich der Fernwärme ein branchenspezifischer Standard definiert. Dieser wurde beim BSI vorgelegt und bestätigt. Die Unternehmen dürfen sich jetzt nach diesem Stand der Technik richten. Der Sinn dahinter ist, dass sie einen Standard haben, an dem sie sich orientieren können, aber es auch eine Breitenwirkung hat, wenn Unternehmen nicht unter die KRITIS-Definition fallen, dass sie dann darauf blicken können und sagen können, was ist Best Practice, was könnte ich machen in meinem Bereich, um vor Angriffen sicher zu sein und mich dort zu schützen. So viel zum Thema KRITIS.

Cybersicherheit für die Gesellschaft

Ich möchte jetzt als letztem inhaltlichem Punkt noch zum Thema *Cybersicherheit für die Gesellschaft* kommen, in dem ich persönlich arbeite. Ich habe vorhin schon einmal den Überblick gegeben über Produkte und Dienstleistungen, die das BSI anbietet. Dort waren beim Thema *Bürger* eher Angebote, die sich direkt an diesen richten. Wir in unserem Referat sprechen eher die organisierte Zivilgesellschaft an und möchten da eher in einen Austausch kommen, um gemeinsam zu gestalten, denn wir sind der Überzeugung, dass wir nicht im Elfenbeinturm sitzen und selbst alles am besten wissen, sondern dort auch in einen Austausch kommen müssen, um Erwartungen, Bedürfnisse und Ideen identifizieren zu können. Und das nicht nur mit dem Staat, nicht nur mit der Wirtschaft, sondern auch eben auch mit gesellschaftichen Akteuren, und am besten sprechen diese auch noch miteinander.

Und deshalb ist dort unser Ansatz das BSI als gesamtgesellschaftlicher Gestalter von Cyber-Sicherheit. Das heißt, wir möchten zum einen eine Plattform bieten für diesen Austausch. Wie auch schon in der Einleitung gesagt, geht es dort um einen Austausch von Staat, Wirtschaft, Wissenschaft und Zivilgesellschaft zu strategischen gesellschaftlichen Themen, um gemeinsam neue Lösungsansätze durch diesen Multi-Stakeholder-Dialog zu erzielen. Wie am Anfang schon sagte, gibt es verschiedene Personen auch hier im Raum, die daran schon teilgenommen haben. Ich möchte darauf auch gleich weiter zu sprechen kommen.

Als zweiten Punkt: mit starken Partnern zusammenarbeiten. Es ist sinnvoll, in verschiedenen Feldern mit Akteuren zusammenzuarbeiten, die vielleicht schon ein spezielles Wissen haben, oder die besondere Befugnis haben. Als Beispiel ist hier die Zusammenarbeit des BSI mit den Verbraucherzentralen zu nennen, weil die Verbraucherzentralen ein sehr gutes Wissen haben, was den Verbraucher angeht, weil sie eine größere Nähe zum Verbraucher haben durch das Beratungsangebot überregional, aber auch bestimmte rechtliche Befugnisse, die das BSI so nicht hat. Und so lassen sich dann diese Befugnisse und Kompetenzen sehr gut kombinieren. Als ein Beispiel der Nutzung dieser Kombination aus Kompetenzen und Befugnissen ist eine Klage anzusehen, die die Verbraucherzentrale NRW erhoben hat, wo es um die Sicherheit von Smartphones geht. Jeder kennt es: Wenn man in einen Elektronikmarkt geht oder online mal nachsieht, was es so für Smartphones im Angebot gibt, beispielsweise Android-Smartphones, dann sieht man, dort gibt es auch noch sehr viele Smartphones mit einem veralteten Betriebssystem, beispielsweise Android 4.1. Als interessierter Nutzer weiß ich: „Veraltetes Betriebssystem! Ich habe da schonmal was von *Stagefright* gehört. Es könnte Probleme mit der Sicherheit des Handys geben!“ Als Laie weiß ich das wahrscheinlich nicht und gehe in den Laden und erwarte ein neues Smartphone, welches funktioniert. Über diesen Umstand informiert der Verkäufer aber nicht: Dass das Smartphone eigentlich ein veraltetes Betriebssystem hat, welches über eklatante Sicherheitsmängel verfügt. Und das, glauben wir, ist ein Umstand, der geändert werden muss und es befindet sich gerade in der gerichtlichen Prüfung, ob der Verkäufer über öffentlich bekannte Sicherheitslücken informieren muss. Und zweitens, ob der Verkäufer auch über den Zeitraum, in dem Sicherheitspatches zur Verfügung gestellt werden, auch informieren muss.

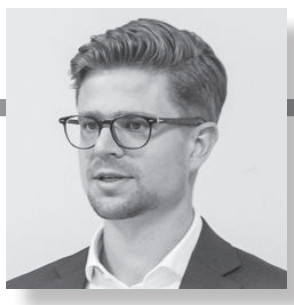
Und drittens wollen wir uns mit Denkfabriken vernetzen, mit Think-Tanks, um auch von außen Input zu bekommen für unsere Arbeit. Um auf diesen Dialog noch einmal konkreter einzugehen, dort haben wir eine Plattform entwickelt: die Denkwerkstatt. Um dort einen vertrauensvollen Dialog zu realisieren, möchten wir uns Zeit nehmen für den Austausch und in einem deliberativen Verfahren gemeinsam neue Lösungsansätze entwickeln. Über diesen breiten Austausch hinaus sind wir gerade dabei, diesen Dialog zu verstetigen, zu vertiefen. Mit einer kleineren Gruppe von Akteuren machen wir uns sehr partizipativ und offen Gedanken, wie wir das gestalten möchten. Nichtsdestotrotz gibt es dieses Modell der Denkwerkstatt weiterhin und läuft im Rahmen eines Projekts.

Desweiteren ist im Kontext der Gesellschaft das Thema des Verbraucherschutzes zu verorten. Dort gab es auch eine Stärkung des Themas durch den Koalitionsvertrag. In diesem wurde konkret dem BSI die Aufgabe des Verbraucherschutzes zugewiesen, und das möchten wir gerne annehmen. Das Ziel ist es, dort Verbraucher so zu unterstützen, dass es eine Sensibilität für diese Themen gibt, sie dann aber auch in ihrer Beurteilungsfähigkeit zu stärken, denn am Beispiel der Smartphones sieht man: der Verbraucher ist oft noch gar nicht in der Lage dazu, Sicherheitsaspekte beurteilen zu können, weil es keine Informationen dazu gibt. Und schließlich, wenn es Unsicherheiten gibt, dann auch Lösungskompetenz zu besitzen, das heißt einerseits, vielleicht zu wissen, wie befreie ich mich aus dieser Unsicherheit oder dann zu wissen, an wen kann ich mich wenden, wer hilft mir. Das ist einerseits natürlich als Beitrag zur individuellen Sicherheit zu sehen, aber auch zur öffentlichen Sicherheit, wenn wir beispielsweise an das *Mirai*-Botnetz denken, das dann auch eine Gefahr für unsere Infrastruktur darstellt.

Schluss

Zum Abschluss zusammengefasst: Cybersicherheit ist eine Bedingung für das Gelingen einer erfolgreichen Digitalisierung. Wir möchten das gemeinsam gestalten für die und mit den verschiedenen Akteuren und wollen für eine sichere digitale Gesellschaft gemeinsam eintreten, dort nicht als Verhinderer angesehen werden, sondern auch als Ermöglicher, denn mit einer sicheren Digitalisierung kann man überhaupt erst diese Digitalisierung bestreiten. Alleingänge sind keine gute Lösung. Es ist eine gemeinsame Verantwortung, und diese Verantwortung gilt es für unterschiedliche Akteure im Dialog und im Austausch wahrzunehmen.

Damit beende ich meine Präsentation und danke für die Aufmerksamkeit und freue mich jetzt auf Ihre Fragen.



Florian Schumacher

Florian Schumacher ist Referent im BSI und leitet dort die Projektaktivitäten im Bereich des gesellschaftlichen Dialogs von Staat, Wirtschaft, Wissenschaft und Zivilgesellschaft zu Fragen der Cyber-Sicherheit. Darüber hinaus koordiniert er die Maßnahmen des BSI im Themenfeld Verbraucherschutz und entwickelt diese strategisch weiter.

Digitale Entmündigung

Verschriftlichung des Vortrags von Rainer Mühlhoff

Die letzten 10 Jahre haben nicht nur den Durchbruch von Smartphones, Cloud-Diensten und Künstlicher Intelligenz gebracht. Zeitgleich ist im Netz eine universelle Infrastruktur zum Sammeln von Bewegungs- und Nutzungsdaten entstanden, der zu entkommen längst auch für versierte User schwierig geworden ist.

Der Beitrag beschäftigt sich mit den gesellschaftlichen Folgen und sozialen Dimensionen dieser Datenaggregation. Eine zentrale Rolle spielt dabei – vielleicht unerwartet – ein genauerer Blick auf die Praktiken des User Experience Designs*. Es werden verschiedene Tricks diskutiert, wie kommerzielle Akteure ihre Nutzer dazu bringen, oft unwissentlich ihre Daten zur Verfügung zu stellen. Es wird diskutiert, wie diese Daten dazu verwendet werden, Nutzerverhalten vorherzusagen und zu beeinflussen. Unter dem Schlagwort* digitale Entmündigung *wird argumentiert, dass es in der aktuellen Netzkultur eine systematische Tendenz dazu gibt, die User ihrer Fähigkeit zum verständigen und selbstbestimmten Umgang mit digitalen Diensten zu berauben. Mit Blick auf die Datenschutzdebatte wird schließlich das politische Problem massenweiser, prinzipiell auch anonymisierter Datensammlung scharfgestellt und es wird auf die Dimension sozialer Ungleichheit und automatisierter Selektion eingegangen, die durch prädiktive Verhaltensanalytik und Profilbildung möglich wird.*

Vielen Dank für die Einladung, es ist mir eine große Ehre hier heute meine Arbeit vorstellen und diskutieren zu können. Digitale Entmündigung ist natürlich ein großer Begriff und ich kann von vornherein sagen, dass ich dazu keine einfache und griffige Definition geben werde. Vielmehr möchte ich unter diesem Label eine Art Zeitdiagnose stellen.

Digitale Technik wird immer relevanter in immer mehr Lebensbereichen, aber zugleich verbreitet sich auch immer mehr eine fatalistische Haltung gegenüber den digitalen Diensten. Man könne oder man wolle die Technik nicht verstehen, geschweige denn sich zum Beispiel der Durchleuchtung der eigenen Privatsphäre erwehren, die großen Plattformunternehmen möglich ist. Diese Resignation verweist auf eine bestimmte Beziehung zwischen technischen Artefakten und ihre NutzerInnen. Diese Beziehung ist allerdings, wie ich jetzt zeigen möchte, heute zum Teil selbst ein Produkt der Gestaltung technischer Geräte, d. h. zahlreiche Aspekte des Designs von Technik wirken darauf hin, NutzerInnen in eine Position der Ohnmacht zu bringen. Die Mechanismen, die das bewirken, und die ich im Ganzen als einen Komplex der digitalen Entmündigung bezeichne, möchte ich im Folgenden anhand von drei zentralen Merkmalen unserer aktuellen Technikkultur umreißen. Das ist

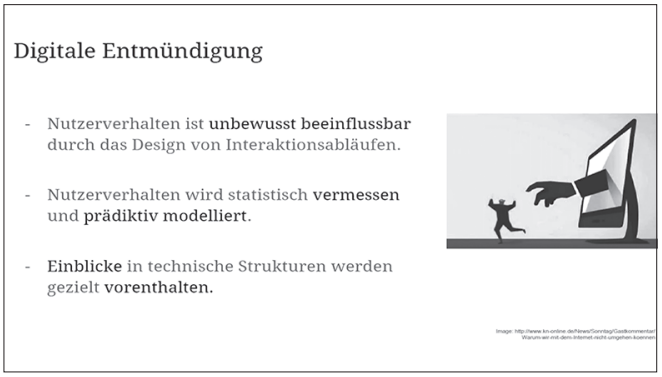
- Erstens: Man geht in der kommerziellen Gestaltung von Interfaces davon aus, dass das Nutzerverhalten unbewusst beeinflussbar ist und zwar durch Stimuli, die im Design von Oberflächen und Interaktionsabläufen liegen,

- Zweitens: Man versucht, die Mechanismen, die dieser Beeinflussbarkeit zugrunde liegen, detailliert statistisch auszumessen und auf diese Weise das Nutzerverhalten prädiktiv zu modellieren,

- Drittens werden Einblicke in die technischen Strukturen, Algorithmen und Plattformen, über die unsere täglichen Interaktionen ablaufen, der durchschnittlichen NutzerIn systematisch vorenthalten.

Im Folgenden werde ich vor allem eine Fülle von Beispielen präsentieren, eine Art Flickenteppich von Aspekten, könnte man sagen, die diese These stützen. Der Punkt ist, dass es sich hierbei um eine Art Gesamtsituation handelt. Es gibt nicht ein einziges Beispiel oder einen einzigen Ursachenfaktor für digitale Entmündigung; vielmehr handelt es sich dabei um ein Zusammenspiel vieler Einzelfaktoren, und ich werde mich außerdem auf Beispiele fokussieren, die in den mehr oder weniger eng umrissenen Bereich des kommerziellen User Experience Designs fallen. Das ist jenes Feld zwischen Informatik, Marketing und Design, in dem die Gestaltung von Mensch-Maschine-Interaktion unter einem holistischen Aspekt betrachtet wird von Usability bis hin zu emotionalen Qualitäten – damit soll aber nicht gesagt sein, dass alle Aspekte von digitaler Entmündigung mit User Experience Design zu tun hätten.

UX ist also nicht der eine große *Bad Guy*, der an allem schuld ist, vielmehr kann man aber an den aktuellen Mainstreampraktiken von UX, den Trend der digitalen Entmündigung ganz gut exemplifizieren.



Ich werde dazu jetzt vier großen Kapiteln vorgehen, die grob mit den drei Thesen der digitalen Entmündigung zusammenhängen, die ich gerade genannt habe.

Interface-Nudges und Design-Tricks

Das erste davon sind die Interface-Nudges. Im Mai wurde auf der Google-Entwicklerkonferenz *Google I/O* das neue *Android P* angekündigt, und da berichtet Spiegel Online: „Die neue

Software soll die Bedienung vereinfachen – und die Nutzer erziehen." Der Guardian titelt, dass Google mit seinem Android P nun Werbung für das *Digital Well-being* mache, und Googles Vice President of Product Management verkündet kleinlaut, dass die Menschen heute damit kämpfen würden, in sozialen Situationen wirklich präsent zu sein, weil Benachrichtigungen auf ihrem Telefon sie zu sehr ablenken würden.

Die kleine kritische Welle im Silicon Valley, die unter Begriffen wie *Time well Spent* oder *Humane Technology* aktuell die Runde macht, scheint also auch bei Google angekommen zu sein, und ganz pflichtbewusst sind im neuen Android P deshalb Funktionen geplant, die die NutzerInnen zu einem Bewusstsein über die Menge an Zeit verhelfen sollen, die sie mit ihren verschiedenen Apps verbringen, und überdies natürlich einen Grund liefern, dass das Gerät diese Zeit trackt und mit einem Google-Server synchronisiert. Außerdem gibt es eine Funktion, die die UserIn daran erinnert, abends ins Bett zu gehen; zum Beispiel verwandelt sich der Bildschirm ab einer voreingestellten Uhrzeit in Graustufen oder die Youtube-App fragt nach, ob man nicht vielleicht eine Pause machen sollte, wenn man länger als eine bestimmte Zeit am Stück Videos geschaut hat.

So etwas sind klassische Nudges, im Sinn des Nudging-Begriffs, der in der Verhaltensökonomik verwendet wird. Nudge heißt wörtlich Stupser, und damit sind kleine, unverbindliche Eingriffe in Entscheidungssituationen gemeint, mit denen versucht wird, das Verhalten der NutzerInnen, vermeintlich zu ihrem eigenen Wohl, zu beeinflussen. Entscheidend für Nudging ist dabei, dass keine Auswahlmöglichkeiten vorenthalten werden, sondern es wird lediglich im statistischen Durchschnitt das Entscheidungsverhalten von NutzerInnen beeinflusst. Nudges operieren dazu über das Design der sogenannten Wahlarchitekturen einer Entscheidungssituation: Das ist die räumliche grafische und interaktive Logik, in der Auswahloptionen präsentiert und aufbereitet werden. Dieser Begriff des Nudging ist aktuell ein ziemlich großer Trend, vor allem im Bereich Public Policy und weil es die User vermeintlich nicht bevormundet, weil es ja keine Option vorenthält, wird es von seinen Advokaten auch als ein Libertärer Paternalismus bezeichnet.

Ein anderes Beispiel für einen Nudge, das aber vielleicht etwas untypischer ist, ist ein Screenshot, der nach dem Login bei Gmail gemacht wurde und der die UserIn dazu auffordert, „Ihren Google-Account abzusichern", indem sie für den Fall eines Passwortverlusts ihre mobile Telefonnummer hinterlegt. Es ist keineswegs davon auszugehen, dass Google allein für diesen Zweck an der Mobiltelefonnummer eines E-Mail-Nutzers oder einer E-Mail-Nutzerin interessiert ist. Interessant ist das Design dieses Dialogs, wo nämlich die Möglichkeit, die Nummer nicht anzugeben, vorhanden, aber gut versteckt ist: Man muss nämlich auf einen kleinen Link unten klicken. Statistisch gesehen ist es völlig klar, dass allein schon aufgrund der grafischen Aufbereitung hier mehr User ihre Nummer angeben werden, als wenn die Auswahlmöglichkeiten einfach gleichberechtigt nebeneinander stünden.

Ein anderes Beispiel betrifft Facebook. Ich verwende jetzt hier einen sehr guten Blogbeitrag von Avi Charkam auf Techcrunch. Wenn man bei Facebook eine externe App benutzen möchte, muss man zustimmen, dass diese App auf die eigenen Profildaten und weitere Daten zugreifen kann, und da hat es von 2011 auf 2012 irgendwann eine Designänderung dieses Dialogs gegeben. In dem alten Design wurde hier links sehr klar gezeigt, dass zwei verschiedene Zugriffsberechtigungen, nämlich auf Basis Profilinformationen und für das Automatische Posten im Namen des Users, an die App vergeben werden, und man auch Zustimmen oder Ablehnen klicken kann, dazu gibt es diese zwei Schaltflächen, die nebeneinander stehen. Im neuen Design wird das ganz anders geframed: Zum Beispiel wird aus den zwei Schaltflächen nur noch eine einzige Schaltfläche. Nach dem *Call-to-Action-Prinzip,* das man aus dem Marketing kennt, mit so einem Imperativ formuliert: *Play Game*, und wenn man die Berechtigung nicht erteilen will, muss man die Seite komplett verlassen, und dann wird z. B. das Wort *Permission* komplett gemieden in diesem grauen Text, der hier in dem neuen Dialog steht, sondern es ist nur noch davon die Rede dass die App bestimmte Informationen erhalten werde. Worum es sich dabei handelt, wird in kleinem grauem Text versteckt und nicht mehr in einer strukturierten Liste mit fettgedrucktem schwarzem Text. Man muss auch erst auf so kleine Fragezeichen gehen, wo dann ein Pop-Up kommt, der das erläutert.

Sehr interessant ist auch das Prinzip der sogenannten *Action Line*, das besagt ganz simpel, man weiß in der Usability, dass Bildschirminhalte unterhalb des niedrigsten klickbaren Objekts ohnehin von der Mehrheit der NutzerInnen gar nicht wahrgenommen werden, und genau hier ist dann das ganze Kleingedruckte in dem neuen Design verkapselt. Das Design dieses Dialogs ist also darauf optimiert worden, dass die User mit hoher statistischer Wahrscheinlichkeit eine Berechtigung zur Datenweitergabe erteilen werden, oftmals, ohne überhaupt bewusst zu begreifen, dass sie dabei Datenzugriffe erlauben. Das Ganze hat System. Wenn man sich ein bisschen damit beschäftigt, dann findet man, dass es einen ganzen Wissenskorpus zu solchen Designtricks gibt. Auch Facebook selbst publiziert auf seiner Homepage für EntwicklerInnen sogenannte *User Experience Guidelines*; darin befinden sich auch Ratschläge, wie man gegenüber UserInnen mit dem Thema der Zugriffsrechte auf Profildaten umgehen soll, zum Beispiel auch, wenn man mit seiner Anwendung oder seiner Website den Facebook-Login benutzen möchte.

Die Seite Pinterest zeigt den Facebook-Login: Zum Beispiel fordert Facebook die EntwicklerInnen von Apps dazu auf, möglichst nicht direkt am Anfang, beim ersten Login oder vor dem ersten Login alle Berechtigungen auf einmal vom User zu erfragen. Stattdessen soll man sich eine Berechtigung immer erst dann einholen, wenn sie im Nutzungsfluss auch benötigt wird, und im Sinne von Datensparsamkeit klingt das ja erst mal ganz gut. Aber zwischen den Zeilen heißt das nichts anderes, als dass die UserIn zunächst mit einem Minimum an Zugriffsrechten in die App gelockt werden soll, um sie zu engagen, und dann macht sie vielleicht aufwändige Dateneingaben oder erstellt sich ein Profil, und wenn man dann noch nach einer weiteren Berechtigung fragt, dann weiß man statistisch gesehen, dass die Wahrscheinlichkeit für einen Abbruch viel geringer ist, als wenn man von vornherein transparent macht, welche Daten die App gerne alles hätte. Ich würde das die Salamitaktik der Datenerhebung nennen.

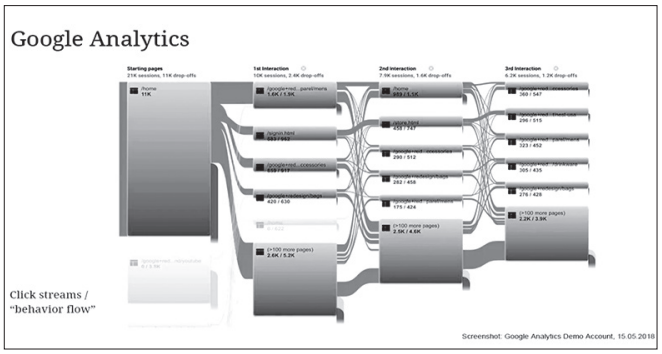
Ich fasse so was unter den Begriff Interface-Nudges. Mit diesem Begriff ist die These verbunden, dass so etwas wie Nudge Thin-

king, das gerade i n Public Policy sehr aktuell ist, auch so etwas wie die dominante Denkweise im *User Experience Design* geworden ist, vor allem im kommerziellen User Experience Design, also das Denken in kleinen subtilen Stupsen, die möglichst unterhalb der Schwelle des Bewussten verlaufen, und entscheidend dafür ist, dass die alternative Wahlmöglichkeit nicht unterbunden oder ausgeblendet, sondern lediglich auf der Ebene großer Nutzerzahlen statistisch unwahrscheinlicher gemacht wird. Das ist aus der Unternehmenssicht das, worauf es ankommt. Dabei kommt keine Technik der Überredung oder Argumentation zum Tragen, sondern grafische Tricks und situative Framings der anstehenden Entscheidung oder der Interaktionsabläufe, die letztlich auf psychologischen oder kognitionsphysiologischen Mechanismen zu beruhen scheinen.

UX-Design und Massendaten

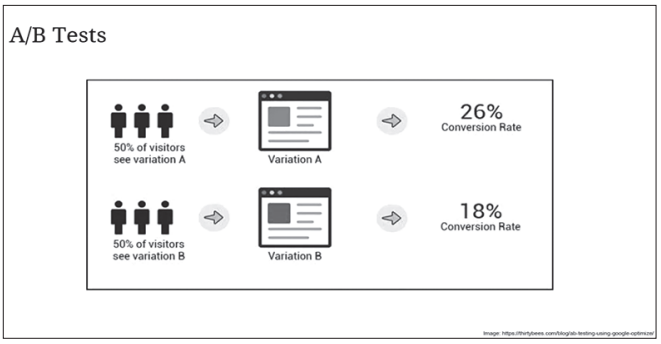
Damit komme ich zum nächsten Kapitel, wie in der Praxis die Auswirkungen eines Interface Designs auf das Nutzerverhalten, also die Effizienz eines Interface Nudges gemessen und empirisch verifiziert werden kann. Es geht jetzt letztlich um die These, dass in der kommerziellen Praxis heute eine inhärente Verbindung von User Experience Design und Massendatenerhebung besteht. Klassischerweise hat man so genannte Usability-Experimente gemacht. Das sind Experimente, für die man Menschen bezahlt, die Webseite oder die Software, die man entwickelt, zu benutzen, darin also bestimmte Aufgaben zu erledigen oder Vorgänge durchzuspielen, und man selber nimmt das dann per Video auf und analysiert es genau. Dabei kann man qualitativ erfassen, auf welche ergonomischen Hindernisse die Person vielleicht stößt, und das macht man dann mit fünf bis fünfzehn zufällig ausgewählten NutzerInnen, um sich ein Bild zu machen. Solche Usability-Tests sind heute immer noch relevant und werden auch immer noch gemacht, aber sie rücken in ihrer Bedeutung deutlich in den Hintergrund, seitdem WebseitenentwicklerInnen fast flächendeckend Web-Analytics-Werkzeuge einsetzen. Das sind Tracking-Techniken, die es erlauben, die Bewegungen jedes einzelnen realen Users im alltäglichen Onlinebetrieb einer Webseite aufzuzeichnen und statistisch auszuwerten. Der Marktführer solcher Werkzeuge ist Google Analytics, das ist ein Service von Google, den man für seine Webseite kostenlos benutzen kann. Dazu muss man nur ein kleines Code-Snippet von Google nehmen und in jeder Unterseite einbinden. Man soll das direkt im Head einbauen, und dieser Code von Google kontaktiert vom Browser des Nutzers aus einen Google-Server, lädt ein paar Javascript-Bibliotheken und meldet auch im Laufe der Session immer wieder ein paar Daten an den Google-Server zurück. Das ermöglicht es Google dann, die Aufrufe der einzelnen Rubriken einer Webseite zu registrieren oder auch die Klicks auf einzelne Links, Buttons oder Bilder, oder wie weit man zum Beispiel die Seite runter gescrollt hat. Für WebseitenbetreiberInnen gibt es dann ein Dashboard, auf dem man zum Beispiel die einzelnen Unterseiten sieht, und wie viele Leute jeweils drauf waren.

Für Usability-Erwägungen sind aber natürlich nicht die einzelnen Seitenaufrufe, sondern eher die Flüsse der NutzerInnen durch die Seite interessant. Dafür gibt es dann auch verschiedene Auswertungsbildschirme, zum Beispiel die Landing Pages, und welcher Anteil von Usern dann als nächstes auf welche der Unterseiten weiter gegangen ist, und wie sich das alles so verzweigt, wie verschiedene User dann durch die Seite wandern. Und da gibt es auch immer diese rot markierten Anteile, das ist der sogenannte Drop-off, also die User die ab hier nicht mehr weiter gemacht haben, weil sie zum Beispiel einfach das Fenster geschlossen haben oder vom Stuhl gefallen sind, und man kann solche Auswertungen auch nach Nutzergruppen, zum Beispiel nach demografischen Kriterien oder nach geografischer Herkunft oder anderen Kriterien differenzieren.



Was für die Entwicklung einer Seite hauptsächlich interessant ist, sind ganz bestimmte typische Nutzerflüsse, das heißt bei einem Onlineshop zum Beispiel von einer Landing Page bis zum Abschluss einer Bestellung, wofür es auch verschiedene Wege geben kann. Man möchte dann wissen, wie viele Leute insgesamt so ein Ziel auch wirklich erreichen; das nennt man im Marketing *Conversion Rate*, also die Anzahl derer, die einen bestimmten Zielpunkt erreichen, relativ zu der Anzahl derer, die vorne angefangen haben. Meistens hat so ein Ziel verschiedene Zwischenstationen, zum beispiel beim Online-Shop *Artikel anschauen*, *Artikel in den Warenkorb klicken*, dann *Zur Kasse gehen*, *Bezahlen*, *Bestellung abschließen* und so weiter. So eine Kette von Schritten nennt man auch *Conversion Funnel*, also Konversionstrichter. Man sieht dabei, dass auf jeder Zwischenstation Leute ausscheiden, und es lässt sich mit einem Analytics Tool auch ganz genau ausmessen, wie viele das sind und welche Nutzergruppen das besonders betrifft, an welcher Stelle. Wirklich spannend wird es jetzt, wenn man sich die Frage stellt, wie man mit dieser Vermessungstechnik denn das Design einer Webseite optimieren kann. Bis jetzt wurde ja nur passiv gemessen, an welcher Stelle und für welche Nutzergruppen vielleicht Reibungspunkte auftreten, aber die Idee solcher automatisierten Analysetechniken beinhaltet ja auch, herauszufinden zu wollen, wie man diese Reibungen reduzieren könnte. Dafür gibt es dann das berühmte A/B-Testing; es ist ein allgemeines Prinzip, für das es auch wiederum von Google einen Service gibt, den man an Google Analytics andocken kann, A/B-Testing ist die Idee, dass man die eigene Seite im Realbetrieb als behaviorelles Echtzeitlabor für Vergleiche verschiedener Designvarianten nutzt. Dazu wird dann randomisiert, zum Beispiel der Hälfte aller Besucher eine Variante A gezeigt und der anderen Hälfte wird eine Designvariante B vorgeführt, die eine kleine Änderung hat. Das kann auch nur ein Teil der Seite betreffen. In dieser Variation sind zum Beispiel bei einem Online-Shop die Preise ein bisschen größer oder eine Schaltfläche ein bisschen blauer oder die Anordnung der Informationen ein bisschen anders, und man kann dann für jede der beiden Varianten separat die Conversion Rates messen. Weil eine Webseite im realen Betrieb typischerweise eine sehr große Nutzerzahl hat, und weil diese Nutzer überhaupt nicht wissen, dass sie an einem Test teilnehmen, erhält man hochsig-

nifikante Erkenntnisse über die relative Effizienz der getesteten Designvarianten. Hier ist eine typische Auswertung von dem an Google Analytics angedockten Tool, wo das Originaldesign gegen vier Varianten getestet wurde. Es wird dann grafisch miteinander verglichen, wie die jeweils performt haben. Die These, die ich hier exemplarisch machen möchte, ist, dass man mit Tracking-Techniken das Internet sozusagen als behaviorelles Echtzeitlabor nutzen kann. Man kann also im großen Maßstab Daten über wahrnehmungspsychologische Verhaltensmuster in Reaktion auf einzelne Designelemente erheben und ausnutzen. Diese Tech-Unternehmen verfügen über ein sehr großes, geheimgehaltenes kommerzielles Wissen über Reaktions-Patterns von Menschen. Das ist vor allem dann bedenkenswert, wenn man auch noch berücksichtigt, dass laut einer Statistik des W3-Konsortiums zwei Drittel der zehn Millionen wichtigsten Seiten im Netz ein Analytik-Tool einsetzen, und darunter ist Google Analytics mit 86 % der Marktführer. Wenn ich das jetzt kurz ausrechne, bedeutet das, dass 56 % der Seiten im Netz Google Analytics einsetzen, und, auch sehr interessant, der zweitbeliebteste Service ist Yandex mit einem Anteil von nur noch 5,2 %.



Die Detailschärfe der Tracking-Möglichkeiten, also dass man auch die Klicks auf einzelne Buttons und Bilder und so weiter erfassen kann, die macht nicht bei den Aufrufen von Unterrubriken halt, und eines meiner Lieblingsbeispiele, dazu komme ich jetzt in einem zweiten großen Beispiel, ist dafür die Google-Suchmaschine selbst. Wenn ich auf der Resultatseite einer Google-Suche etwas anklicke, dann wird dieser Klick an den Google-Server zurückgemeldet. Wenn ich zum Beispiel in meinem Firefox nach *Aktuelle Nachrichten* suche, dann kommt bei mir als erstes Resultat die Tagesschau und der Link sieht im HTML dann so aus: Da ist wohl bemerkt dass korrekte Zielangebot gegeben – tagesschau.de – aber es gibt da noch das Javascript-event *onmousedown*, welches eine funktion *rwt* mit ziemlich vielen Parametern aufruft. Diese Funktion rwt – das steht übrigens wenig verhohlen für *rewrite* – ist oben im Kopf des Dokuments definiert, und die macht nichts anderes als die Ziel-URL des Links im Moment des Klicks auszutauschen. Wenn man den Mausbutton wieder loslässt, ruft die NutzerIn also mit diesem Klick die ausgetauschte URL auf. Diese führt zu einem Google-Server, der schnell diese ganzen Parameter registriert und dann mit einem HTTP-status-code-302-Mechanismus auf die ursprünglich gewünschte Seite weiterleitet. Was genau in diesen Parametern alles drin steht, ist ein gut gehütetes Betriebsgeheimnis. Man kann nur ein bisschen was mit Backwards-Engineering rausfinden. Ich habe das mal versucht, zum Beispiel wird erfasst, welche Position das angeklickte Resultat auf der Seite hatte und es wird eine eindeutige Suchsession-Nummer mit übertragen. Besonders pikant finde ich, dass es auch einen Parameter gibt, der erfasst, ob man mittels des Zurück-Buttons oder über das Umschalten zwischen Tabs auf die Resultate-Seite zurückgekommen ist, nachdem man sich schon ein anderes Resultat angeschaut hatte. In Kombination aus diesen drei ersten Parametern kann Google also ganze Such- und Klickhistorien tracken und so statistisch auswerten, welches Resultat vielleicht zufriedenstellender war als ein anderes. Auch noch spannend der letzte Parameter, er ist nämlich nur dann vorhanden, wenn man einen Google-Account-Cookie hat, also wenn man in einem anderen Fenster bei Google eingeloggt ist, zum beispiel in Gmail oder Youtube. Das erlaubt es dann, diese gesamte Suchhistorie auch noch dem konkreten Nutzer zuzuordnen. Google benutzt dieses detaillierte Click-Tracking auf seiner Resultate-Seite natürlich, um seine künstliche Intelligenz für die Ermittlung relevanter Suchresultate zu trainieren. Die unfreiwillige Einhegung von Menschen zur Gewinnung von Trainingsdaten für KI wäre noch einmal ein anderes Vortragsthema, auf das ich jetzt hier allerdings nicht näher eingehen kann. Worauf es mir hier ankommt, ist, dass durch das detaillierte Tracking klassische Usability-Messinstrumente durch massendatenbasierte Auswertungen ersetzt werden können. Um zu ermitteln, welche Elemente auf einer Seite am meisten wahrgenommen werden, würde man als klassisches Usability-Experiment z. B. Eye-Tracking-Studien machen.

Der Punkt ist, dass der Click-Tracking-Mechanismus mit diesen ganzen detaillierten Parameterauswertungen erlaubt, äquivalente Auswertungen täglich und in Echtzeit zu machen, ohne dafür Leute extra vor einen Rechner setzen zu müssen, und ohne dass die Probanden überhaupt davon wissen.

Google Search Click Tracking Mechanismus

cd=1	Position of result on the SERP list
ved=0ahUKEwjj5t3t0YLZAhULlSwKHb-eAYcQFgguMAA	Search session ID + Type of result (organic, ad, knowledge graph, image, maps, …)
cad=rja	Returning via back-button / tab switch?
url=http://www.tagesschau.de/	Tagret URL
usg=AOvVaw1_8NtrWpEbLefVcTd78eDR	Signed target URL (fraud detection)
sig2=LG.....h-s....	Google Account ID (logged-in users)

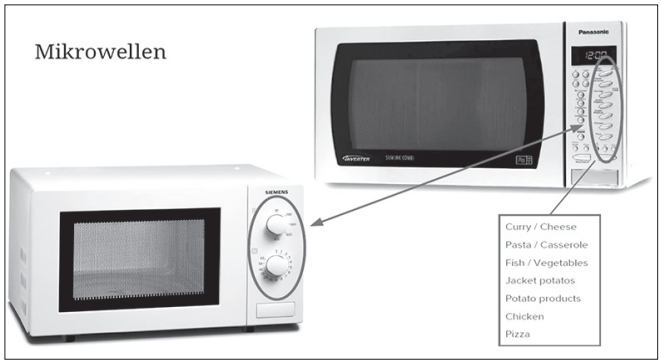
Vgl. Mühlhoff (2019). "Big Data is Watching You"

Ich habe jetzt zwei Beispiele für Tracking etwas ausführlicher besprochen, aber es ist wichtig, dass es sich dabei um die Gesamtsituation handelt, in der verschiedene Technologien Hand in Hand gehen. Insbesondere gibt es neben Analytics Services noch viele weitere, sehr verbreitete Strukturen, die eine statistische Auswertung von Nutzerbewegungen im Netz gestatten. Darunter sind der Facebook-Like-Button, die Login-Dienste von Google und Facebook sowie verschiedene Tracking-Cookies und Web-Beacons und vieles mehr zu nennen, worüber man hier auch jeweils sehr ausführlich berichten könnte. Hier geht es mir um die Gesamtschau: Darin zeigt sich, dass das Tracking vom Zweck der Usability-Optimierung sicherlich nur ein Teilaspekt von etwas viel größerem ist. Vielleicht ist es allerdings der Aspekt, über den sich das Tracking ziemlich gut verbreiten konnte, denn der Zweck der Designoptimierung ist ja für Webseiten-EntwicklerInnen ein ziemlich wichtiges Anliegen. Web Analytics Services sind also vielleicht ein ganz guter *Social Hack*, um über die Mitwirkung von Webseiten-EntwicklerInnen eine flächendeckende Trackinginfrastruktur zu etablieren. Deswegen sind sie vielleicht auch kostenlos. Worauf ich mit dieser Betrachtung hinaus möchte, ist, dass es heute eine inhärente Verbindung von

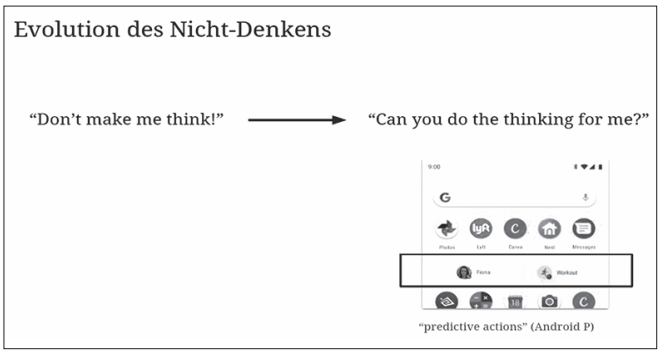
UX-Design und Massendatenerhebung gibt. User Experience Design, wie es industriell betrieben wird, ist eine massendatenbasierte Wissenspraxis, das heißt, die Begriffe und Denkweisen, der Denkstil, die Wissensbasis und die Designziele, die in diesem Feld eine Rolle spielen und diskutiert werden, also der ganze Wissenskorpus, werden durch die Sammlung und Auswertung von Verhaltensweisen wesentlich beeinflusst und mitproduziert.

Versiegelte Oberflächen

Nach diesen sehr aktuellen und anwendungsbezogenen Überlegungen will ich in dem dritten Kapitel jetzt noch etwas allgemeiner werden und ein wenig herauszoomen. Es gibt in der Evolution der Mensch-Maschine-Interaktion über die letzten Jahrzehnte – damit meine ich jetzt so zwei bis drei Jahrzehnte – eine Entwicklung, die ich als den Trend der versiegelten Oberflächen bezeichnen möchte. Ich werde das entlang von zwei Dimensionen hier entfalten: das eine ist die Dimension des Denkens und das andere die Dimension des Verwaltens. Das hier ist eine Staubsaugerdüse, sie hat so einen Schalter, um auszuwählen, ob man eine borstige oder eine glatte Düse verwenden möchte. Das hier ist meine zweite Staubsaugerdüse, die hat auch wieder diesen Schalter. Diese Düse ist etwas neuer, die Bebilderung des Schalters hat sich verändert, im alten Design wird die Eigenschaft der Düse borstig oder glatt gezeigt, und in dem neuen Design geht es um die Eigenschaft des Bodens. Die Düse sieht im neuen Design jeweils gleich und unspezifisch aus, während der Boden einmal glatt und das andere mal haarig ist. Ganz aktuell ist übrigens noch dieses dritte Design, das ich gefunden habe, da ist auf dem Schalter gar keine Düse mehr skizziert, sondern nur noch ein Symbol für Parkett versus Teppichboden. Eine ähnliche Beobachtung kann man bei Mikrowellen machen: Da gibt es auch zwei Designvarianten für das Bedieninterface, einmal wo man die Dauer und die Leistungen einstellt, und da, wo man zwischen solchen Lebensmittelprogrammen wählen kann: Pasta Chicken Curry und so weiter, und es wird dann nach irgendeinem opaken Rezept auch nur über den zweiparametrigen Raum von Dauer und Leistungen selektiert. Meiner Meinung nach ist dieser Unterschied fundamental: Man erschafft mit den neueren Designs nämlich eine Interaktion, in der es nicht mehr darum geht, das Gerät in seinem mechanischen Aufbau zu erfassen. Der NutzerIn wird es in den neueren Designs nicht ermöglicht, das Gerät in einer Zweck-Mittel-Relation einzusetzen, die sich durch Denken und Wissen über seine Funktionsweise erschließt, sondern der denkende und verstehende Schritt wird ihr abgenommen und die Interaktion mit dem Gerät kreist nur noch darum, direkt den Endzweck auszuhandeln, nämlich was sie sagen will oder erwerben möchte. Das ist dem Gerät dann überlassen, wie genau dieser Zweck erfüllt wird und es ist bedauerlich, dass man die Staubsauger dann noch selber durch den Raum führen muss.



Man möchte nicht denken müssen – könnte man auch sagen – und damit führt die Assoziationskette auf diesen netten Buchtitel, *Don't make me think*, von Steve Krug, das war in den 2000er Jahren ein Standardwerk zum Thema Webdesign und Usability. Steve Krug spricht vom Prinzip *don't make me think* als der Usability-Regel Nummer eins. Damit meinte er damals allerdings noch ein bisschen bescheiden, dass man einem Objekt zum Beispiel sofort ansehen muss, ob es klickbar ist oder was sich dahinter verbergen wird, wenn man drauf klickt, so dass man bei der Benutzung nicht durch Momente des Grübelns oder Rätselns unterbrochen wird. Natürlich ist das eine ziemlich gute Sache, denn manch ein wirklich schlechtes Design von manch einem Nerd oder einer Nerdin krankt sehr genau an dieser Stelle. Aber meine These ist, dass sich dieses Prinzip mittlerweile und vor allem durch das kommerzielle Betreiben über die ursprünglichen Usability-Erwägungen hinaus zu einer kulturell codierten Gewöhnung ans Nicht-Denken-Wollen verselbstständigt hat.



Wenn man diese Evolution des Nicht-Denken-Wollens extrapoliert, würde ich sagen, dass man heute auch gar nicht mehr in der Ära des *Ich will nicht denken* ist, sondern des *Can you do the thinking for me*, das sieht man an so vielen kleinen Details des viel beworbenen *Predictive Actions-Bar* im neuen Android P; das ist hier diese rot markierte Zeile, wo das Telefon rät, was Du als nächstes machen möchtest und das Dir schon so anzeigt als Schaltflächen bis hin zur Google-Suche, die die Antworten schon anzeigen möchte, bevor man überhaupt eine Frage eingibt. Die zweite Dimension der versiegelten Oberflächen habe ich mal Verwalten genannt. Beim guten alten Dateimanager von Windows 3.11 sieht man ganz übersichtlich die einzelnen Laufwerke, das Gerät und daneben den Verzeichnisbaum, der sich darin befindet. Der Windows-Explorer kam mit Windows 95. Man kann hier zwar immer noch auf die einzelnen Laufwerke des Rechners zugreifen, aber es gibt eine zusätzliche Ebene, hier ganz prominent, die eher sowas wie einen prozessgeleiteten Zugriff auf Dateien ermöglicht. Man zeigt da besonders relevante Ordner an, die dann aber nicht über ihren strukturellen Ort im Dateisystem selektiert werden, sondern als Shortcut dienen. Man geht davon aus, dass es sich dabei um für die meisten User besonders relevante Orte handelt, die man dann schnell und ohne viel Nachdenken findet. Der Apple Finder wurde danach erst so richtig populär, der kann das alles auch was die beiden vorher gezeigten Dinger konnten, aber hier kommt noch mal eine Funktionalitätsebene hinzu: Der Finder ermöglicht nämlich den Zugriff auf Objekte- durch Suchinteraktion. Damit rückt dann ein prinzip von Frage und Antwort in den Vordergrund, also ich interagiere,

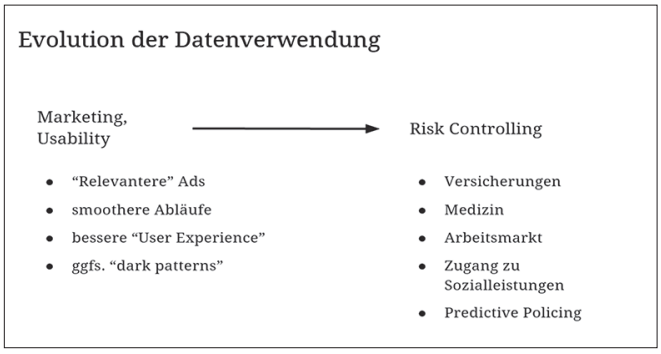
indem ich eine Suchanfrage stelle, und kriege die Objekte dann angezeigt. Das heißt, man greift plötzlich auf Dateien zu, völlig ohne über ihren strukturellen Ort auf dem System bescheid wissen zu müssen, zu. Wenn ich das nebeneinander stelle, ist das eine bemerkenswerte Evolution vom Verwalten über das Explorieren bis hin zum Finden, und ich denke, wir leben auch heute schon gar nicht mehr im Zeitalter des Findens sondern des Pickens. Das Wort *Picker* ist in der Smartphone-Welt die Bezeichnung für so einen kontextsensitiven Auswahldialog, da man keinen Zugriff auf Laufwerke, sondern man bekommt situativ das angezeigt, was mit größter Wahrscheinlichkeit gerade relevant ist und was in den Kontext passt. Man muss dann aus einer Shortlist von Alternativen nur noch etwas herauspicken. Übrigens haben iPhones überhaupt kein Interface mehr, um auf die eigentliche Verzeichnisstruktur des Geräts zugreifen zu können. Alle Dateien, die den User etwas angehen – sagt der Entwickler oder die Entwicklerin – werden in der iCloud synchronisiert, und das entspricht ja dann einer virtuellen Datenstruktur, nicht der Art und Weise, wie die Dateien wirklich auf dem physischen Gerät abgelegt sind. iPhones sind also die ersten Geräte, die für den Zugriff auf den physischen Speicher, der sich darin befindet, kein User Interface mehr anbieten. Eine bemerkenswerte Entwicklung, die es sicherlich auch nicht ohne weiteres gegeben hätte ohne die Vorgeschichte die das hatte – und das ist eine Vorgeschichte von User Experience Design, an dem Apple seit den 1980er Jahren maßgeblich beteiligt ist.

Ich möchte solche Entwicklungen unter dem Begriff der *Versiegelten Oberflächen* zusammenfassen. Es handelt sich dabei um den Trend, die Technizität technischer Artefakte hinter bunten und anthropomorphen Oberflächen zu verkapseln. Zwei Merkmale sind dafür kennzeichnend.

- Erstens: Man will nicht oder man traut den Usern nicht zu, dass sie das Gerät instrumentell benutzen, das heißt als Werkzeug, dessen technische Eigenschaften sie kennen und dessen Verwendbarkeit sich durch Denken erschließt, und

- Zweitens: Man will nicht oder man traut den Usern nicht zu, die Fähigkeit oder den Willen zu besitzen, die interne Organisation eines Geräts strukturell zu erfassen.

Man scheint eher zu denken, dass der durchschnittliche User oder Userin immer in einen Nebelfeld mit maximal einem Schritt weiter Sicht steht; deshalb muss man ihm immer genau das vor die Nase halten, was für den nächsten Schritt die relevanten Auswahlmöglichkeiten sind, und alle anderen Optionen blendet man aus. Die theoretische These, die hier dahinter steckt, ist, dass Technikgestaltung als eine Art Sozialisationsfaktor aufgefasst werden muss. Damit meine ich, dass das Design von Mensch-Maschine-Interaktion eine Rückwirkung hat auf die Menschen und ihre Fähigkeiten. Die Grundidee der Usability, dass nicht die Menschen sich dem technischen Gerät, sondern die Technik sich den Menschen anpassen soll, die stimmt zwar und hat uns auch weit gebracht, aber sozialtheoretisch ist sie falsch, denn sie suggeriert einen einseitigen Prozess, wo aber tatsächlich es sich um eine Wechselwirkung handelt, denn die Interaktion mit Technik formt Gewohnheiten und Wahrnehmungsweisen. Sie prägt die Art und Weise, wie man technische Geräte erlebt, intuitiv mit ihnen interagiert, sie begrifflich repräsentiert, über sie diskutiert, den ganzen Denkstil und die Praktiken, die damit zusammenhängen. Als Gedankenexperiment stelle man sich nur einmal vor, im Jahr 1995 ein Smartphone von 2018 in die Hände zu bekommen. Wäre man damals in der Lage gewesen, das zu bedienen und vor allem zu erfassen, was da passiert? Die Sozialisationswirkung oder technischer gesagt Subjektivierungswirkung, von der ich hier spreche, betrifft dann natürlich auch die Resignationshaltung, dass man Technik ja sowieso nicht verstehen könne oder wollte, und ihr seht, worauf das jetzt hinausläuft. Ich behaupte, dass das was industrielles User Experience Design als eine Annahme über die Menschen in ihre Überlegungen hineinsteckt, in Wirklichkeit ein Produkt dieser Technikkultur ist, die dieses User Experience Design mit hervorbringt. Natürlich ist die Idee, dass man technische Geräte einem größeren Nutzerkreis zugänglich macht, indem man sie vereinfacht, eine grundlegende Kulturtechnik seit jeher schon. Ohne sie wären die meisten technischen Artefakte für viele überhaupt nicht zugänglich deshalb ist Usability auch nicht generell schlecht. Doch die Sache ist ambivalent, denn sie wird in dem Moment destruktiv, oder sie kann in dem Moment destruktiv werden, wenn Vereinfachung zur Bevormundung wird, indem Informationen und Beeinflussungsmöglichkeiten systematisch weggeblendet werden. Im Umkehrschluss heißt das dann, dass eine ermächtigende Gestaltung von Benutzer-Interfaces auch empowerte User hervorbringen kann, und zu einem solchen Design würde gehören, interne Abläufe sichtbar zu machen, wenn man sie sehen will. Einstellungsmöglichkeiten anzubieten, wenn man sie sucht, Komplexität nicht hinter infantilisierenden Bildern und simplizistischen Benennungen zu verkapseln sondern sachlich zu benennen, und es wäre ein separater Vortrag, so etwas wie emanzipatorische User Experience Guidelines mal genauer auszuführen.



Um langsam in Richtung eines Schlusses zu kommen, möchte ich noch einmal an die Interface-Nudges aus dem ersten Abschnitt erinnern. Was man daran sieht, ist, dass Nutzerverhalten als beeinflussbar gilt und zwar – das ist wichtig – durch prereflexive Stimuli und subtile Eingriffe in den Interaktionsverlauf. Dann haben wir im zweiten Kapitel gesehen, dass das kommerzielle Internet dicht besiedelt ist mit Messeinrichtungen, um die Reaktionen der User auf solche Stimuli quantifizieren zu können. Der Mensch gilt also nicht nur als unbewusst beeinflussbar, sondern in seinem Verhalten auch noch als statistisch modellierbar. Der Punkt ist jetzt, dass hiermit nicht gesagt sein soll, dass immer nur von einer einzigen typischen Reaktionsweise oder Verhaltensweise von Menschen ausgegangen wird, denn die Menschen sind verschieden, und das wissen auch Big-Data- und Usability-Experten. Was man mit Big-Data- und Deep-Learning-Techniken machen kann, ist, Profilgruppen von untereinander ähnlichen Nutzern zu bilden, also das Verhalten nach Typen einzuteilen, und spätestens seit Cambridge Analytica ist

es niemand mehr entgangen, dass sich die Profilbildung, die man auf Grundlage von Massendaten erreichen kann, die man auf Social-Media-Plattformen erhebt, sich nicht nur darauf bezieht, ob jemand eher auf blaue oder rote Schaltflächen klicken würde, sondern anhand der Daten, die gerade im Social-Media-Bereich aggregiert werden können, auch Metriken entwickelt werden, die User hinsichtlich ihrer affektiven Reaktion kategorisieren oder hinsichtlich ihrer politischen Manipulierbarkeit, hinsichtlich ihrer Sucht- und Krankheitsdisposition, Lebensführung, Kaufkraft und Kreditwürdigkeit etc. Das heißt, Tracking-Daten werden, wo sie schon einmal da sind, nicht nur zu Usability-Zwecken eingesetzt, sondern haben längst viel lukrativere Monetarisierungsstrategien gefunden. Wie es ein niederländischer Privacy-Aktivist formuliert, denken die meisten User zwar immer noch, ein kostenloser Service im Internet werde durch Werbung finanziert, und wenn Nutzerdaten dann dazu genutzt werden, bessere Werbung anzuzeigen, dann ist denen das auch vielleicht recht. Der Punkt ist aber, dass der Markt für die Verwertung von aggregierten Verhaltensdaten sich aktuell vom Marketing zum Risikomanagement verschiebt. 2017 war das erste Jahr, wo das Marktvolumen für Risikomanagement-Produkte größer war, als das für Marketing. Risikomanagement bedeutet, prädiktive Modelle auf Grundlage von Massendaten dazu zu verwenden, Menschen algorithmisch in Risikokategorien einzuteilen. Solche Modelle können z. B. von Kfz- oder Krankenversicherungen dazu benutzt werden, kundenindividuelle Versicherungspreise zu berechnen, je nach Prognose über ihren Fahrstil oder Gesundheitszustand, oder bei Job-Bewerbungen werden Menschen anhand algorithmischer Vorhersagen über ihre erwartbare Performance vorsortiert, die man zum Beispiel anhand von Daten auf E-Learning-Plattformen an Universitäten meint, ableiten zu können, die man sich irgendwo einkauft oder anderweitig gewinnt. Big-Data-basierte Modelle werden in den USA dazu verwendet, den Zugang zu sozialstaatlichen Ressourcen und Sozialleistungen wie Medicaid, Obdachlosenunterstützung oder Altenheimplätze zu regulieren, und nicht zuletzt werden solche Modelle auch für die prädiktive Polizeiarbeit eingesetzt. Dieser Übergang vom Marketing zum Risikomanagement bedeutet nichts anderes, als die kommerzielle Verbreitung algorithmischer Techniken der sozialen Selektion, des Managements von Armut und Krankheit und, wie viele KritikerInnen argumentieren, der Zementierung bereits bestehender gesellschaftlicher Ungleichheitsverhältnisse.

Schluss: Kollektiver Datenschutz

Das bringt mich zu dem letzten Punkt, dass zu einem politischen Weg aus der digitalen Entmündigung auch eine Debatte um kollektiven Datenschutz gehört. Nach aktueller Gesetzeslage werden die meisten Trackingdaten legal erhoben und verarbeitet. Die Datenschutzgesetzgebung, obwohl sie in Deutschland und neuerdings auch in der Europäischen Union weltweit eine der strengsten ist, bleibt einer individualistischen Perspektive verhaftet. Das schützenswerte Gut sind die personenbezogenen Daten des Einzelnen, darunter fallen diese Trackingdaten aber oft gar nicht, und außerdem erlaubt das Gesetz, jedem Individuum, der Erhebung dieser Daten freiwillig zuzustimmen und das geschieht ja dann unter dem Prinzip *Informed Consent* in den allermeisten Fällen. Damit fallen aber die gesellschaftlichen Folgen dieser Datensammlung komplett durch das Raster der Privacy-Debatte. Es wird nicht bedacht, dass die Verwendung meiner Daten auch anderen Menschen schaden kann, denn auch die Person, die selbst nichts zu verbergen hat und deshalb ihre Daten hergibt, trägt zur Gesamtheit der Datenpunkte bei, auf deren Grundlage andere Individuen negativ bewertet oder diskriminiert werden können. Auch wenn ein privilegierter Erdenbürger selbst keine negativen Auswirkungen dadurch spürt, dass Google seine E-Mails hat oder Facebook über sein Sozialleben bescheid weiß, trägt er mit diesen Daten dazu bei, dass andere Menschen aufgrund ihrer E-Mails und aufgrund ihrer Facebook-Präsenz als Abweichler, als Hochrisiko-Kunden, als psychisch labil, als gerade für diese oder jene Sache empfänglich oder eventuell als gefährlich selectierbar sind. Die negativen Konsequenzen der Datennutzung sind also nicht auf alle Mitglieder einer Gesellschaft gleich verteilt, sondern treffen die Armen, Schwachen, Kranken und Minderheiten überproportional. Das liegt natürlich daran, dass prädiktive Modelle im Zeitalter von Künstlicher Intelligenz nicht mehr so funktionieren, wie die alten Credit-Scores, wie zum Beispiel der Schufa-Score, die jedes Individuum anhand seiner eigenen Vergangenheit bemessen, sondern Massendaten-basierte Metriken beruhen auf statistischen Vergleichen zwischen vielen Individuen, wodurch Leute anhand von Verhaltensähnlichkeiten, die zum Beispiel auch in ganz anderen Lebensbereichen liegen können, in Gruppenhaft genommen werden, und das heißt, der Kern der digitalen Entmündigung im Zeitalter von KI- und Trackingdaten liegt nicht primär darin, dass das einzelne Individuum immer transparenter wird, sondern dass alle Individuen auf Grundlage von Pattern Matching bloß noch als Exemplare von Typenprofilen aufgefasst und dann unterschiedlich behandelt werden. Zu einem mündigen Umgang mit digitalen Geräten gehört deshalb eine Besinnung auf kollektive Daten und Schutzinteressen, die nicht bei der autonomen Verfügung über die eigenen Daten stehen bleibt, denn anders als es das Wort *Privacy* suggeriert, ist es eben keine Privatsache, wie man mit seinen Daten umgeht, ob man sie für sich behält oder freiwillig preisgibt, sondern tatsächlich handelt sich dabei um eine hochpolitische Angelegenheit. Vielen Dank.

Rainer Mühlhoff

Rainer Mühlhoff ist wissenschaftlicher Mitarbeiter am Sonderforschungsbereich *Affective Societies* an der Freien Universität Berlin. Der Schwerpunkt seiner philosophischen Forschungen liegt im Bereich Sozialphilosophie, Affekt-Theorie und kritische Theorie der digitalen Gesellschaft. Er studierte Mathematik, theoretische Physik, Philosophie und Gender Studies in Heidelberg, Münster, Leipzig und Berlin.

Künstliche Intelligenz: Theoretische Grenzen, praktische Möglichkeiten und der politische Diskurs darüber

Verschriftlichung der Podiumsdiskussion mit Aljoscha Burchardt, Constanze Kurz und Karen Ullrich

Wem nützt KI überhaupt, was stellen die Firmen und Staaten damit an, dazu diskutieren jetzt Karen Ullrich, die ihr gerade schon kennen gelernt habt im Vortrag, Aljoscha Burchardt ist Computerlinguist am Deutschen Forschungsinstitut für Künstliche Intelligenz, da ist er, und moderieren wird Constanze Kurz, Informatikerin, Sprecherin des CCC, ihr kennt sie.

Constanze Kurz: Während jetzt alle noch verkabelt werden, werde ich ein paar Sätze sagen zu unserem Plan, den wir gemacht haben, über den wir reden wollen. Ich glaub wir haben ein bisschen Einblick bekommen, wie man heute aus wissenschaftlicher Sicht daran geht, aber wir wollen natürlich das Thema Künstliche Intelligenz ein bisschen breiter debattieren, aus mehreren Gründen. Zum einen, weil es, das kann man schon sagen, ein Hype-Thema ist, gerade in Deutschland in den letzten Monaten, weil wir einen Vertreter mit Aljoscha auf dem Podium haben. Das ist deine Seite. Weil wir einen Vertreter mit Aljoscha auf dem Podium haben, der gestern gerade bei der Eröffnung der KI-Enquête im Deutschen Bundestag war, darüber werden wir auch ein bisschen sprechen. Wir werden über die anderen Kommissionen, Parlaments- und Regierungskommissionen sprechen, und warum das Thema Künstliche Intelligenz mit all seinen Facetten derzeit so populär ist in der Politik. Wir werden natürlich auch einen Aspekt besprechen, der in diesem Vortrag noch keine Rolle gespielt hat, aber, glaube ich, für die Entwicklung der KI von ganz entscheidender Bedeutung sein wird, nämlich die finanziellen Anreize, die hinter den verschiedenen Systemen stehen, und warum deshalb auch so relativ kontrovers darüber gesprochen wird. Wir wollen aber keineswegs, haben wir uns zumindest nicht vorgenommen, nur über die Risiken reden, sondern selbstverständlich versuchen, möglichst facettenreich abzubilden. Ich will vielleicht mal anfangen mit Aljoscha, weil er gestern in der Eröffnungssitzung der Enquête war, ich will noch ein paar Sätze sagen zu der Enquête, nur um sie abzugrenzen von den anderen Kommissionen, mit denen jetzt Aljoscha nichts zu tun hat. Die Enquête-Kommission ist dem Wortlaut nach eine Untersuchungskommission, sprich, der Bundestag, und zwar nur der Bundestag, nicht die Regierung, möchte sich beraten lassen von Experten. Und die Enquête-Kommission, wie alle Enquête-Kommissionen davor, sind paritätisch besetzt zwischen Abgeordneten und Sachverständigen, und Aljoscha ist ein Sachverständiger, weil er als Nicht-Abgeordneter dazukommt. Die anderen Kommissionen, wie insbesondere der Digitalrat, der ist bei der Bundeskanzlerin angesiedelt, wird auch zu KI mit beraten, oder die Daten-Ethik-Kommission, sind keine parlamentarischen Kommissionen, sondern gehören zur Regierung. Wir haben eigentlich sogar noch eine vierte, die sich mit dem Thema beschäftigt, nämlich der nationale Ethikrat, der auch teilweise Künstliche Intelligenz in seinen Besprechungen drin hat, und warum das so ist, dass sich so viele Kommissionen damit beschäftigen, darüber wollen wir ein bisschen reden. Aber vielleicht sagst du mal, Aljoscha, wie war es denn gestern, und inwiefern können wir als Fußvolk an dieser KI-Enquête teilnehmen?

Aljoscha Burchardt: Also das war übrigens ein Thema, inwieweit das Fußvolk teilnehmen kann. Gestern konnte man teilnehmen,

die erste Sitzung war öffentlich, die wurde im Parlamentsfernsehen übertragen, aber da ist natürlich noch nicht viel passiert, da haben sich dann 38 Leute vorgestellt. 19 Parlamentarier und 19 Sachverständige, das ist eine bunte Mischung, also die Parlamentarier selber, die kommen natürlich aus den unterschiedlichsten Professionen. Das sind Leute mit wirtschaftlichem Hintergrund, mit juristischem Hintergrund, theologischem Hintergrund, was auch immer, und das selbe gilt eben auch für die Experten. Eigentlich waren die eher Technik-Experten, so wie ich, und dann eben auch Experten aus der Zivilgesellschaft, die sich mit Netzpolitk beschäftigen, oder auch mit theologischen Fragen, alles mögliche. Also ein wirklich bunt gemischter Haufen, und warum man die eingesetzt hat, das ist ein großes Thema, das die Bundesrepublik Deutschland wie alle anderen Länder auf dieser Welt für viele Jahre beschäftigen wird. Die Idee ist eben, man schlaut sich gemeinsam auf und versucht abzustecken, was drin ist, auch mal zu definieren, worüber man redet, ein Stück weit auch die Ängste zu nehmen, und zu versuchen, die Chancen zu finden, aber auch die No-Go-Areas zu finden, dass man sagt, es gibt da eben auch Vorbilder, international, denen wir nicht folgen wollen, und so weiter. Das ist der Rahmen.

Constanze Kurz: Ich werde gleich mal Karen fragen, was sie sich eigentlich wünschen würde, was so ein Untersuchungsgegenstand sein sollte, bevor ich dich frage, was tatsächlich inhaltlich beschlossen wurde. Aber ich hab noch ein paar organisatorische Fragen dazu. Wird es Arbeitsgruppen geben, und werden die auch in der Zukunft zugänglich sein?

Aljoscha Burchardt: Es wird Arbeitsgruppen geben, das wird demnächst am 14./15. Oktober in einer Klausurtagung dann noch einmal besprochen, welche das geben soll. Es ist immer abwechselnd, es gibt immer eine Sitzung der Obleute, das ist von jeder Partei einer, das ist so ein kleines Gremium, was erst

mal die grobe Richtung macht, und dann wird immer die große Kommission zusammengerufen. Dann gibt es diese Untergruppen tatsächlich, aber das ist noch nicht klar, zu welchen Themen die geschnitten werden, also ob die nach Ressorts geschnitten werden, nach Technologien geschnitten werden, nach Anwendungsbereichen, das muss noch ausgehandelt werden. Und es wurde diskutiert, ob diese Sitzungen öffentlich sein sollen, das ist noch Streitthema; die Grünen haben sich sehr stark dafür gemacht, dass jede Sitzung öffentlich sein soll. Andere Parteien hatten zum Teil eine gespaltene Meinung, ich glaube, es war niemand grundsätzlich gegen Öffentlichkeit, aber ich muss selber sagen, also ich bin auch öfter mal mit den Grünen überein, inhaltlich, das würde ich gar nicht verhehlen, aber in diesem Punkt, finde ich, man muss nicht immer öffentlich tagen, weil es auch sein kann, dass man über inhaltliche Sachen sich erst mal unterhalten will, dass sich vielleicht auch Politiker mal outen müssen, oder ich als Wissenschaftler mal was sagen können muss, ohne dass mein Chef am Fernseher das mitbekommt. Also ich finde es schon okay, wenn man sich eben auch mal hinter verschlossener Tür unterhält, und dann jede x-te Sitzung wieder öffentlich macht, oder wenn man gefunden hat, mit welcher Message man nach draußen gehen soll, du sitzt ja auch nicht bei Coca Cola mit dabei, wenn die die Marketing-Strategie machen, aber okay, wir sind hier nicht bei Coca Cola.

Constanze Kurz: Naja, ob man jetzt ein Wirtschaftsunternehmen wie Coca Cola mit dem Deutschen Bundestag vergleichen will, na gut, aber vielleicht sollten wir es mal offen legen, die Sachverständigen sind jeweils immer von einer Fraktion benannt, und alle Fraktionen des Deutschen Bundestags sind vertreten, und zwar paritätisch. Für welche Fraktion bist du denn da der Sachverständige?

Aljoscha Burchardt: Ich bin also von der FDP vorgeschlagen worden, aber ich selber bin parteilos, also sozusagen wirklich als Wissenschaftler da, mir selbst verpflichtet.

Constanze Kurz: Und formal, ich war ja selbst mal Mitglied einer Enquête-Kommissionen eines früheren Bundestages, ist man natürlich als Sachverständiger auch unabhängig. Jetzt frage ich mal Karen, was würdest du dir eigentlich wünschen, wenn du – natürlich, es ist ein politischer Prozess, und die werden sich da auch beharken, insbesondere dann, wenn es aktuelle Gesetzgebungsprozesse geben könnte, in gesetzgebenden Ausschüssen, die da auch reingrätschen – aber was würdest du dir eigentlich wünschen, was so eine den Bundestag und damit auch zukünftige Bundestage beratende Kommission in diesem breiten Feld, wo du eben so ein paar Themen schon angerissen hast, betrachtet und untersucht? Was würdest du dir da eigentlich vorstellen wollen?

Karen Ullrich: Also, ich würd mal vorausschicken, dass das jetzt vielleicht meine Meinung ist, also als Privatperson, und dass es relativ unabhängig ist von mir als Wissenschaftlerin, ich als Privatperson, was ich als Privatperson oder als Wissenschaftlerin, seit 2012 erlebe, in der sich das abgezeichnet hat, dass die Algorithmen so viel Erfolg haben, ist, dass Industrie sehr schnell sehr viel Geld in diese Themen steckt, und im Endeffekt dann auch sehr viel Macht ausübt. Es ist seit 2012 also ein Spiel um Macht, wer eigentlich welche Talente bekommt und welche Patente und welches Wissen, und diese Systeme am schnellsten umsetzen und anwenden und ausnutzen kann. Und was man so ein bisschen sieht, sind zwei große Spieler, die Betriebe in den USA, Google, Facebook, nvidia, und der zweite große Spieler, muss man auch ganz klar sagen, ist China, und dann stellt sich so ein bisschen die Machtfrage, will ich jetzt alle Macht sozusagen übergeben an einen Staat, der das wie auch immer nutzt, wie das in China passiert, oder gebe ich alle Macht an so Betriebe wie Google und Facebook, also wo ist der Mittelweg. Ich denke, das ist eine der zentralen Fragen, die man sich ja eigentlich vor 5 Jahren hätte stellen müssen, wenn man mal ehrlich ist.

Constanze Kurz: Nun hat der Deutsche Bundestag wenig Möglichkeiten, auf Technologiekonzerne in Asien oder Amerika zuzugreifen, er kann ja erst mal nur, vielleicht mit europäischen Partnern, wenn er eine europäische Regelung anstrebt, gewisse Grenzen setzen oder auch Untersuchungsgegenstände anpeilen und den Ist-Zustand erst mal in seinen Bericht schreiben, über den er was aussagen kann und den er vielleicht später regulieren kann.

Karen Ullrich: Ich meine aber auch ganz konkret, einfach zu sagen: Ich nehme Geld in die Hand als Staat oder als Europa vielleicht. Aber Menschen, Ingenieure, Wissenschaftler sind heutzutage sehr mobil und vielen von meinen Kollegen, ist das relativ egal ob die in Europa arbeiten, ob die in Deutschland arbeiten oder in den USA arbeiten. Das Wissen, was ich erschaffe, ist ja nur zu so einem ganz kleinen Teil Macht, die ich dann einem großen Konzern gebe und man muss schon ganz einfach sagen: Also die Arbeitsbedingungen – zumindest an meiner Universität – die sind nah an katastrophal, und meine Kollegen rennen zu den großen Betrieben, die – ohne Übertreibung – fünf bis zehn Mal so viel bezahlen. Also, ich muss ganz einfach sagen, viele meiner Kollegen, die sind passionierte Wissenschaftler und da geht's gar nicht darum, um die Arbeitsbedingungen, das viele Geld, aber oft auch einfach um die Sicherheit, dass es keine Festanstellung gibt und so etwas. Und das ist eine Politik, die zum Beispiel Kanada nicht fährt, also einige von meinen Kollegen, die heute in Kanada leben, am Vektorinstitut zum Beispiel, da ist eine Riesen-Initiative, da dann forschen.

Constanze Kurz: Also damit wäre es ja dann eine forschungspolitische Forderung. Ich habe jetzt ein extensives Nicken auf Aljoschas Seite gesehen. Wir haben vorher besprochen, dass wir durchaus ein bisschen über Geld reden wollen. Aljoscha arbeitet beim DFKI, das ist ja eine Institution, die prinzipiell einen besonderen Schwerpunkt im Drittmitteleinwerben hat, insofern ist jetzt dein Nicken nicht so furchtbar überraschend, aber ich glaube die gesamte Strategie, die wir bei der Bundesregierung sehen und auch das ungefähr zwölfseitige Papier, was gerade so rauskam von der Regierung in Bezug auf die Förderung – KI ist ja ein reines forschungspolitisches Blatt, wenn man so will. Aber würdest du das auch als zentralen Punkt dieser Arbeit sehen, wenn du jetzt auf diese ganze Enquête blickst?

Aljoscha Burchardt: Nein, aber ich stimme nur zu, bei uns das ja ganz genauso, wir leben eben auch von Fördergeldern, das DFKI kriegt keine Grundfinanzierung, wir müssen das Geld alles sozusagen auf dem freien Markt, in den Förderprogrammen oder eben für die Industrieaufträge einwerben. Für uns gilt auch so ein Besserstellungsverbot, also wir dürfen nicht mehr als irgendwelche Ministerialbeamten verdienen, das wird da genau so gedeckelt, und im Silicon Valley werden die KI-Größen wie Fußballstars gehandelt und du bietest denen hier ein Grund-

schullehrergehalt an als Junior, also das ist schon wirklich ein bisschen, ähm, interessant als Idee. Aber ich weiß nicht, in der Enquête wird es sicherlich auch darum gehen müssen, was man in den Forschungstopf rein tut, da waren ja auch die großen Ideen, mit Deutschland/Frankreich zusammen was zu tun, wo die Bundesregierung dieses Jahr zwar nicht so wahnsinnig viel Geld eingestellt hat und für das nächste Jahr ein paar hunderttausend Euro, aber damit holt man ja nicht, was man sich auf die Fahnen geschrieben hat, den Wettbewerb in China und den USA wieder auf. Aber wenn ich jetzt vielleicht wirklich noch einmal das Fass ein bisschen aufmachen darf, welche Chancen wir eigentlich haben, wir werden nicht mehr Facebook und Google werden, aber ich bin auch der Meinung, jetzt wirklich als Wissenschaftler, dass wir – wir haben ja bisher nur über maschinelles Lernen gesprochen –, dass wir eigentlich mit diesem sehr datenhungrigen Ansatz im Moment, wenn man in der Geschichte der KI guckt, die niedrig hängenden Früchte erntet. Es gab ja früher auch andere Ansätze der KI, wissensbasierte Expertensysteme, wo man wirklich versucht hat, hands-on das Wissen in der Maschine zu modellieren. Wolfgang sagte immer, warum soll man die Naturgesetze jetzt aus Daten lernen, die sind ja da. Man kann sie ja vielleicht der Maschine auch anders beibringen, das ist aber natürlich ein Riesen-Thema. Aber wir haben ja in Deutschland hier den starken Mittelstand, unsere Ingenieurskunst, wir haben ja auch Bildungstradition, worum uns die anderen Länder beneiden, China hat sehr viel Geld, zum Teil aber auch noch nicht die Talente, die wir hier haben, und die Leute sind vielleicht nicht so mobil, dass sie alle gern nach China gehen, in die USA, das ist völlig anders, die Firmen sitzen ja auch zum Teil hier in Berlin. Aber ich würde mir erhoffen, dass wir auch forschungsmäßig und inhaltlich vielleicht was dagegen setzen können, weil man tut immer so, als wenn das Rennen schon gemacht wäre, aber ich glaub da ist auch noch forschungsmäßig viel drin, vielleicht nicht so datenhungrig, transparenter, eher wissensbasiert und dann eben auch mit unseren ethischen Standards und unseren Datenschutzstandards, die wir gern hätten, aufgebaut. Da denke ich, können wir auch eine neue Qualität erzeugen, das mag jetzt vielleicht wissenschaftlich naiv klingen, aber ich würde hoffen, dass uns das glückt, wenn wir sozusagen frohen Mutes an die Sache herangehen. Aber wir dürfen nicht mehr wahnsinnig lange warten, eine ganze Menge Geld in die Hand zu nehmen, und wenn ich mir den Rüstungshaushalt angucke, dann wäre doch ein ähnlicher Haushalt für Bildung und Forschung ganz schön, ja.

Constanze Kurz: Ach ja, da wären wir beim Thema. Die Wahrscheinlichkeit, dass irgendein Militärforschungsaspekt in dieser Enquête, die die KI betrachten soll, überhaupt besprochen wird. Also gibt es irgendeine Wahrscheinlichkeit dafür, dass da auch die ethisch richtig problematischen Grenzbereiche besprochen werden?

Aljoscha Burchardt: Kann ich schlicht und ergreifend noch nicht sagen. Ich kann es mir vorstellen, aber es kann auch sein, dass es herunterfällt, aber ich kann es einfach noch nicht sagen. Aber das ist natürlich ein wichtiges Thema, selbst wenn man sich auf die Fahnen schreibt, dass man es nicht tun will. Das DFKI zum Beispiel hat auch einen Beschluss: Wir machen keine militärische, keine „kriegerische" Forschung, vielleicht beim hinterher Aufräumen und Helfen und Retten, aber keine kriegerischen Einsätze, aber, man muss ja auch davon ausgehen, dass es andere auf der Welt gibt, die das nicht so sehen, und die so Zeug entwickeln. Man muss sich vielleicht auch dem stellen, man muss zumindest mal up-to-date bleiben und sagen, was da gemacht wird und wie man sich ggf. auch wehren kann, aber so weit würde ich dann auch gehen. Irgendeine Stellung muss man zu der Bedrohung beziehen.

Constanze Kurz: Ich will mal ein bisschen wegkommen von dieser Enquête, ich meine das können wir vielleicht beobachten, sicherlich nicht so zeitnah wie du, aber wir werden als Öffentlichkeit irgendwie daran teilhaben können. Gestern haben einige der Parlamentarier schon gesagt, dass es zumindest regelmäßige Berichte gibt, die kann man sich ja dann ansehen, und vielleicht für diejenigen, die sich auch für diese Bestandsaufnahme interessieren, die ja am Beginn immer der Enquête ist, wird es vielleicht ganz interessant, weil man das Feld der KI in etwas breiteren Facetten abbilden kann. Aber ich will mal auf die größere Diskussion in der Bevölkerung kommen. Mir scheint, es ist jetzt so drei, vier Jahre ein größerer Hype, aber zumindest in den deutschen Diskussionen, man kann es vielleicht sogar für die europäische sagen – ich hab das kürzlich im europäischen Parlament mal kennen gelernt – ist es eine eher angstbehaftete Diskussion, sie ist geprägt so ein bisschen von dieser kommerziellen Auswertung von maschinellem Lernen, die insbesondere mit USA-Beispielen gespickt ist, Ihr habt im Vortrag ja selber einen gebracht, und jetzt in letzter Zeit, noch mit China-Beispielen, die immer noch ein Stück gruseliger sind, zeichnet das für das Forschungsfeld eigentlich ein akzeptables Bild? Oder ist es so überzogen mittlerweile, und hat sich gelöst von der Diskussion in der Akademia, wie die Öffentlichkeit darüber spricht und wie diese Befürchtungslage, die mir immer größer scheint, eigentlich ist? Wie würdet ihr das abgleichen?

Karen Ullrich: Ich denke, das ist ja im Prinzip auch eine juristische Frage, ich glaube woraus häufig die Angst besteht, ist, dass wir viele Sachen einfach noch nicht ausgehandelt haben, also ich muss Informatikern ja nicht erzählen, dass der Besitz bei Algorithmen ein sehr strittiges Thema ist, also das Patentrecht, und das macht auch eigentlich überhaupt keinen Sinn bei Produkten, die wir eigentlich für null Kosten produzieren können. Zumindest muss das komplett überholt werden, und es wird selbst in diesem uralten Thema nicht überholt, und jetzt haben wir dieses neue Feld, was wieder ganz andere, im Endeffekt Machtfragen, aber auch juristische Fragen stellt. Wem gehört die Verantwortung, wenn was schief geht? Welche Rolle spielt derjenige oder der Datenserver, auf dem der Algorithmus läuft, der die Voraussagen gibt? Wem gehört das Modell, das vielleicht auf Daten basiert, die mir aber nicht gehören? Kann ich Daten entleihen, kann ich Modelle entleihen? Also wie funktionieren solche Sachen, das sind eigentlich Dinge, die ganz zentral, eigentlich sehr juristisch ausgehandelt werden müssen, meiner Meinung nach. Und wenn das nicht passiert, dann kommen eben schlechte Akteure oder halt Akteure, die das ausnutzen für ihre eigenen Zwecke, auf eine ganz große Bühne, und das ist schon etwas, wovor man auch berechtigt Angst haben muss.

Constanze Kurz: Wir haben ja ein paar Bereiche, da wird das noch kommen, da wird es in Europa kommen, da wird es in Deutschland kommen, möglicherweise wird die Enquête darüber beraten, aber wir haben auch einige Bereiche, da ist das schon passiert. Ich will vielleicht mal ein Beispiel nennen: In der letzten Legislatur hatte das Verkehrsministerium ja ein Gesetz gemacht

für selbstfahrende Autos, oder auch assistiertes Fahren, und sozusagen das erste Mal so eine Haftungsfrage, die ja letztlich über Software entscheidet, festgelegt, nämlich zu Ungunsten des Fahrers oder desjenigen, der drinsitzt, teilweise sind die Entscheidungen ja schon passiert. Und zwar auch in einem Bereich, in dem man jetzt nicht unbedingt die Techniker fragt, sondern das war ganz sicherlich eine Entscheidung pro Auto-Industrie. Go ahead.

Aljoscha Burchardt: Bevor wir auf das autonome Fahren – das ist ja immer ein super Thema, mache ich auch gern – aber noch ein Satz zu dem davor. Ich habe in Deutschland den Eindruck, dass im Moment so ein bisschen der Schwanz mit dem Hund wedelt. Wenn man so mit den Politikern spricht, die denken alle, „müssen wir machen", Digitalisierung, total wichtig, KI ist der Schlüssel zur Digitalisierung, ich sage mal es hat so ein bisschen was von DDR, „überholen ohne einzuholen". Also wir wollen jetzt den richtigen, den großen Push, jetzt haben wir 30 Jahre geschlafen mit der Digitalisierung, aber KI macht das jetzt, jetzt kommen wir wieder an die Weltspitze. Aber dann siehst du, wenn du in die Bevölkerung guckst – wirklich breite Teile der Bevölkerung, auch in meiner Familie und überall – die Leute haben Vorbehalte, auch mit gutem Grund, die SPD-Leute wegen Arbeitsplätzen, die Grünen wegen Datenschutz, die Leute von der CDU „brauchen wir net, hatten wir gestern auch net", die von der FDP sagen, die Auftragsbücher sind voll, die Maschine rollt, ich hab keine Fachkräfte, warum soll ich denn jetzt digitalisieren? Also alle sind sich sozusagen unten an der Basis einig, das ist blöd und das wollen wir nicht, und das ist dann natürlich auch ein großer Blocker, Geld in die Hand zu nehmen. Wenn du jetzt Geld in die Hand nimmst, dann geht das Gejammer los: Die Infrastruktur und die Rentenversicherungen und die Brücken sind kaputt und so weiter. Du hast ja sozusagen erst Mal eine Kommission zu gründen. Das finde ich ja auch prima, rede ich ja gerne mit, aber ich denke das ist im Moment die Situation, die wir in Deutschland haben: Eine irgendwie geartete Technikaufgeschlossenheit, dass alle sagen, yay, cool, wir kriegen smarte Homes, wo man vielleicht länger autonom zu Hause bleiben kann, wegen autonomer Autos, die uns vielleicht sicherer und Energie sparender durch den Verkehr bringen und andere Dinge, die irgendwie eine positive Vision darstellen. Man kann immer beide Seiten angucken, mache ich auch wirklich gerne. Aber davon sehe ich so gar nichts. Ich bin dann immer auch als Erklärbär unterwegs und versuche auch die andere Seite mal zu zeigen.

Constanze Kurz: Na, immerhin gibt es dieses Papier, das wir vorhin schon mal kurz angesprochen haben. Bevor diese Enquête ins Leben gerufen wurde vom Parlament, gab es ja ein Regierungspapier, und interessanterweise, das erste, worauf man guckt, ist immer, naja, welche Ministerien haben dieses Papier gemacht, also diese 10, 12 Seiten. Also das war das Forschungsministerium und das Wirtschaftsministerium, und so ist es auch ausgefallen. Es geht ja im Wesentlichen um Geld, und das liest sich auch sehr angstvoll, finde ich, man merkt ganz doll, da steckt viel Angst drin, auf diesen Zug nicht mehr aufspringen zu können, man will da jetzt auch ein bisschen Geld reinstecken, aber auch wieder nicht so viel, hmm. Das ist ja so ein bisschen wie eine Vorlage, die ihr jetzt bekommen habt, und die, finde ich, auch nichts damit zu tun hat, was in den Zeitungen über KI steht, wo ja vor allen Dingen die verschiedenen Formen von ganz praktischer Diskriminierung, oder aber auch von Nichtwissen darüber, wie jemand hinter meinem Rücken über mich entscheidet, gar nicht auftauchen, sondern dass es wirtschaftspolitisches Förderungsprogramm gesehen wird. Da ist ja irgendwie so ein Disconnect aus meiner Sicht zwischen dem was geforscht wird, auch was man objektiv wissen kann, über maschinelles Lernen, und was so die Bevölkerung befürchtet.

Aljoscha Burchardt: Das stimmt, wenn ich nochmal darf, jetzt bringst du mich noch mal auf das Stichwort Disconnect. Bei uns in der Forschung, ganz konkret, bei uns in der Sprachtechnologie, Leute in meiner Gruppe, arbeiten daran, die Eigennamenerkennung in Texten zu verbessern, vielleicht von 70% Precision auf 80% zu kommen, und dafür müssen 80.000 Dokumente von Hiwis annotiert werden, und da müssen die Algorithmen nachtrainiert werden und so weiter und so fort, das sind Aufgaben, damit beschäftigt man sich. Andere Kollegen in der Robotik versuchen, die Übergabesituation, der Roboter gibt dir was in die Hand, er darf es dir nicht auf den Fuß fallen lassen, er darf es erst loslassen, wenn du es hast, solche Dinge werden in der Forschung erforscht, und da wird viel gemacht, da gibt es tolle Erfolge, aber das ist so weit weg jetzt eben von den Visionen, die Leute haben mit Killer-Robotern und Überwachungsstaat und man denkt, das ist so wie der Genmais, ja, ein Mal aufs Feld geschmissen fliegt der in alle Winde, und wenn wir einmal die KI haben, dann haben wir als nächstes was ganz Schreckliches. Das ist wirklich, glaube ich, ein Disconnect, zwischen dem, was zum Teil in der Forschung gemacht wird und eben auch diese dusseligen Anwendungen, die wir da aus den USA sehen. Was Google da gemacht hat mit diesem Anrufcomputer, der da irgendwie die Öffnungszeiten abfragt oder so, das sind, finde ich, sozusagen für deutsche Seelen, dusselige Anwendungen, das finden wir nicht schön.

Constanze Kurz: Es ist jetzt für dich eine schlechte Frage, weil du das ja schon tust, indem du den Bundestag versuchst zu beraten. Aber, was kann man eigentlich tun, wenn man tatsächlich in dem Feld arbeitet, um diese merkwürdige Situation aufzulösen, ohne aber gleichzeitig in so ein Hurra-Geschrei auszubrechen. Da kommen Probleme auf uns zu, die brauchen wir hier, glaube ich, unter Informatikern auch nicht weiter besprechen. Aber wie kann man eigentlich dazu beitragen, dass es ein bisschen versachlicht wird, oder dass man vielleicht auch die Aspekte, die in Deutschland wirklich gerade beforscht werden, wo wir gut drin sind, mal hervorhebt?

Karen Ullrich: Also ich denke, die Frage, die man sich vielleicht stellen muss, wenn man davon spricht, dass es so als – wie hast du es gerade bezeichnet? – als Wirtschaftsprogramm gesehen wird, also wo genau stellen sich denn Leute die Wertschöpfung vor, die von solcher Forschung ausgehen kann? Und ich denke, die ist sehr viel vielfältiger. Was wir jetzt vielleicht in den letzten fünf Jahren primär gesehen haben, ist ja quasi die Nachahmung von menschlicher Wahrnehmung, also wir gucken uns ein Bild an, wir wissen, da ist eine Katze drauf, und wofür man das alles nutzen kann. Und allein da haben wir schon gesehen, wie wahnsinnig viel Geld das spart, es funktioniert Spracherkennung. Es funktioniert, das heißt wir können Call-Center loswerden, es spart uns viel Geld, das ist eine Form von Wertschöpfung. Es ist einfach nur faktisch – das ist noch nicht mal eine Kritik – das Benennen und das Konkretmachen: Das führt einfach dazu, dass Leute wissen, worüber man eigentlich konkret redet, also wo es Geld dafür gibt. Leute zu ersetzen, die ganze Automatisierung ist natürlich meiner Meinung nach nicht so schrecklich, weit weg

und wird ja auch schon gemacht mit den Algorithmen, also das ist eine Sache. Ich denke in der ganzen Robotik, da ist man – also eigentlich alles, was echte mechanische Systeme sind – realistisch gesehen echt noch weit weg. Man redet dann wirklich von so einem Roboterarm, der gerade einen Turm bauen kann. Dass der irgendwie ganze Mechanik oder so ersetzt, ich glaube das ist noch in absehbarer Zeit so nicht möglich. Ich kann jetzt einfach mal so Sachen benennen, was Google X so macht, das ist die Forschungsgruppe in Google, die so die außergewöhnlichen Forschungsprojekte haben, also die beschäftigen sich z. B. auch mit Ernährung, wie können wir mehr und mehr Menschen ernähren, wie können wir KI dazu nutzen, dass Pflanzen besser wachsen, wie können wir vielleicht in solchen künstlichen Gewächshäusern eine ganz andere Qualität von Pflanzen schaffen, wie können wir vielleicht Gentechnik beschleunigen mit KI, so etwas zum Beispiel. Ernährungssicherheit, da geht es darum, wie können wir herausfinden, an welchen Standorten wir aufgrund von geophysikalischen Daten noch irgendwelches Erz herausholen können und mit dem Vorsprung an Wissen die Rechte an solchem Land kaufen. Ein Riesenversprechen, das in dem Sinne auch noch nicht eingelöst werden kann, liegt in der Medizin, eine ganz große Hürde wäre das Immunsystem zu verstehen und daraus neue Medikamente zu entwickeln, da gibt es schon vielfältige Forschungsansätze. Was ich immer extrem finde, dass, wenn ich jetzt von solchen Sachen erzähle, sind fast alle von denen ausschließlich in diesen riesigen Firmen präsent.

Aljoscha Burchardt: Ein Punkt, der mir auch immer wichtig ist, um so aus diesem Sammel- und Angstbegriff mal wieder ein bisschen wegzukommen, wirklich sich genau zu überlegen, worüber redet man? Redet man wirklich nur über digitalen Wandel, Digitalisierung? Die Tatsache, dass wir online Bücher kaufen, gar keine Bücher mehr kaufen, und der Buchhandel kaputt gegangen ist, das hat jetzt nichts mit KI zu tun.

Constanze Kurz: Es ist ja schon hin, weil ich dachte die Buchmesse wird die größte ever.

Aljoscha Burchardt: Aber sagen wir mal, ich kenne die kleinen Buchhandlungen in unserer Umgebung, manche von denen hatten es schwer. Ich wollte nur sagen, das ist Digitalisierung, dass natürlich dann auch große Firmen irgendwo KI einsetzen, um Recommender zu machen oder für die Übersetzung, oder um ihre Kunden zu clustern und die besser bedienen zu können, gut, da kommt dann Machine Learning rein, aber nicht jede Form von Machine Learning würde ich jetzt auch gleich als große KI bezeichnen, das hilft den Leuten auch nicht weiter. Und dann, das hilft dann auch ein bisschen, wenn man das ein bisschen auseinander zerrt, weil viele Leute haben schlicht und ergreifend keinen Bock auf digitale Transformation, digitalen Wandel, und das kann man auch so diskutieren, aber dann braucht man nicht über KI zu reden, dann muss man nicht immer das große Fass anstechen. Aber ein Punkt, der mir wichtig ist: Wir versuchen eben immer, auch Projekte zu machen, man muss auch ein bisschen Werbung machen, ich habe gerade ein Buch herausgegeben: „IT für soziale Inklusion“; das könnt ihr euch open access herunterladen, umsonst. Da haben wir viel Mühe hineingesteckt und Arbeit, auch mal Beispiele zu geben, für solche Anwendungen, die eben die Leute integrieren, die noch heute gar nicht integriert sind, D21 hat diesen Digitalindex, der gibt den immer heraus, 19% der deutschen Bevölkerung, jeder Fünfte ist noch nicht überhaupt online, in keinster Weise, kann keine Öffnungszeiten nachgucken.

Aljoscha Burchardt, Constanze Kurz und Karen Ullrich

Aljoscha Burchardt ist Leiter des Sprachtechnologielabors des *Deutschen Forschungszentrums für Künstliche Intelligenz* (DFKI GmbH). Er ist Experte für Künstliche Intelligenz und Sprachtechnologie. Zu seinen Interessen gehören die Bewertung der (maschinellen) Übersetzungsqualität und die Einbeziehung von Sprachexperten in den MT R&D-Workflow. Burchardt ist Mitentwickler des MQM-Frameworks zur Messung der Übersetzungsqualität. Er hat einen Hintergrund in semantischer Sprachtechnologie. Nach seiner Promotion in Computerlinguistik an der Universität des Saarlandes koordinierte er das Forschungsexzellenzzentrum *E-Learning 2.0* an der Technischen Universität Darmstadt. Burchardt ist stellvertretender Vorsitzender der Berliner Wissenschaftlichen Gesellschaft.

Constanze Kurz ist promovierte Informatikerin, Autorin und Herausgeberin mehrerer Bücher, aktuell zum Cyberwar. Ihre Kolumne *Aus dem Maschinenraum* erscheint im Feuilleton der FAZ. Sie ist Aktivistin und ehrenamtlich Sprecherin 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 und im Beirat des FIfF.

Karen Ullrich ist Doktorandin an der Universität von Amsterdam und Alumni des *Austrian Research Institute for AI*. Sie forscht zum maschinellen Lernen und interessiert sich für die achtlose Anwendung der Algorithmen und oft unbewußte Beeinflussung von Nutzerinnen und Nutzern.

Sie sind überhaupt nicht online, das wird sich auch mit der Zeit ändern. Ich will nicht die Technik in die Leute integrieren, sondern tatsächlich auch Leute, die unsere Sprache nicht verstehen, die vielleicht auch nur leichte Sprache verstehen, die sich nicht orientieren können im Raum vielleicht Hilfen brauchen beim Gehen, oder um irgendwo hinzukommen, oder die wissen müssen, wo ein Fahrstuhl ist, und so weiter. Wir haben ja viele „wirkliche" Integrationsprobleme, die man auch technologisch angehen kann. Und dass man versucht, auch einen guten Mix hinzubekommen, auch für diese Projekte kriegt man ja Fördermittel, und da gibt es auch Fördergeber, die man finden kann, zum Teil kriegt man auch Sponsoring. Das haben wir auch schon geschafft, als damals die große Flüchtlingssituation war, 2015, 2016, da haben dann auch Leute unsere Übersetzungs-App, die wir dann gebaut haben, gesponsort. Wenn man sich ein bisschen bemüht, kann man eben auch versuchen, solche Projekte immer umzusetzen. Damit kann man auch nicht allein seine Butter aufs Brot kriegen, aber das kann man auch machen.

Constanze Kurz: Na gut, es sind im Prinzip ähnliche Antworten. Eine gewisse Betonung, dass die Forschung nicht immer nur am Profit und der Profilierung eines großen Tech-Konzerns dienen soll, sondern sehr viel mehr Facetten hat. Das wäre sozusagen eine der Antworten. Aber dann sind wir eigentlich schon wieder bei der forschungspolitischen Frage, weil wir ja einfach wissen, dass die Summen, die in maschinelles Lernen und angrenzende Bereiche investiert werden, von den Proportionen her sehr unterschiedlich sind. Im Bereich der universitären Forschung etwa, wenn man das mit Deutschland vergleicht, oder eben auch was die großen Konzerne vor allem in Asien eine riesengroße auch schriftlich festgehaltene KI-Strategie haben, von fast monströsen Ausmaßen, oder eben, was die amerikanischen Konzerne da reinstecken. Vielleicht ist das der Punkt, an dem man – gerade weil die Bundesregierung in ihrem eigenen Strategiepapier, wo sie die „Sprunginnovation" ja gern hätte – so sehr diesen forschungspolitischen Aspekt betont, dass man ehrlicherweise sagen müsste, dass diese albernen Summen, die sie da vorschlagen, natürlich nur ein Tropfen auf dem heißen Stein sind, Und dass es letztlich – das muss man leider auch für das DFKI sagen, aber sicherlich auch für deine Forschungseinrichtung – fast keine Universität gibt, die nicht im Wesentlichen mit diesem Drittmitteleinwerben zu tun hat. Drittmittelgeber, wenn man sich das in Europa zumindest mal ansieht, sind natürlich auch in großem Maße amerikanische Tech-Konzerne. Das ist leider ein Fakt, der sich über die Jahre eher noch verstärkt als weniger wird. Ich glaube aber, dass es Forschungspolitik allein nicht sein kann …

FIfF-Konferenz 2018

Die DSGVO: Eine kommentierte Reise durch die (Un-) Tiefen des juristischen Feuilletons – eine launige Bilanz nach vier Monaten Geltung

Verschriftlichung des Vortrags von Kirsten Bock und Malte Engeler

Vom Foto-Verbot zum Ende strukturierter Visitenkartensammlungen. Vom großen Blogsterben zu Zahnärzten und ihren Datenschutz-Tonbandansagen. Von überforderten Aufsichtsbehörden zu jubelnden Silicon-Valley-Riesen: Die DSGVO hat all den bekannten Kontroversen des Datenschutzrechts neuen Diskussionsstoff gegeben. Die Twitter-Szene hat die großen, kleinen (und vermeintlichen) Aufreger dankend aufgegriffen. Kirsten Bock und Malte Engeler begeben sich anhand ausgewählter Tweets auf eine kommentierte Twitter-Reise durch die Untiefen des DSGVO-Wahnsinns.

Herzlichen Dank nochmal ans FIfF, wir freuen uns ganz besonders heute hier sein zu dürfen. Wir möchten kurz darauf hinweisen, dass wir privat hier sind und nicht für unsere jeweiligen Dienststellen hier stehen. Das gleiche gilt für die Tweets, die wir hier aufnehmen. Auch diese nehmen wir zur Anschauung, wir folgen denen nicht und bewerten sie auch nicht.

Hier heute beim FIfF zu sein, ist uns besonders wichtig, weil der Mensch im Mittelpunkt stehen soll. Das ist ein Aspekt der in den Diskussionen um die Digitalisierung häufig viel zu sehr in den Hintergrund gerät. Und wenn wir uns mit der DSGVO befassen, dann wollen wir das heute auch besonders vor diesem Hintergrund tun: Den Menschen nicht aus den Augen zu verlieren.

Wie haben wir uns das also vorgestellt? Wir sind beide sehr aktiv auf Twitter und haben uns angeguckt, was seit vier Monaten – seitdem gilt die Datenschutzgrundverordnung – eigentlich so in der Szene diskutiert wird. Dafür haben wir uns repräsentative Tweets herausgefischt. Natürlich ist das auch ein wenig Beispiel unserer eigenen Filterblase. Wir haben versucht, die Debatte ein bisschen divers aufzustellen, aber nochmals der Hinweis: Wir nehmen auf gar keinen Fall den Standpunkt ein, es sind einfach Spotlights in der Diskussion, nicht unbedingt unsere eigenen Auffassungen. Teilweise schon, aber nicht immer.

Da wir auf öffentlich gemachte Tweets von Personen zurückgreifen, haben wir uns tatsächlich auch die Frage gestellt: Dürfen wir das eigentlich, dürfen wir lauter Tweets mit Bildern, mit Namen, mit Twitter-Handles an die Wand werfen und hier in den Köpfen und im Stream speichern lassen? Wir haben uns ziemlich den Kopf zerbrochen, ob das überhaupt zulässig ist.

Also haben wir uns auf die Suche nach der berühmten Rechtsgrundlage gemacht. Das ist immer der erste Schritt, wenn man weiß, was für Daten man verarbeitet. Das hatten wir schnell eingegrenzt: Tweets mit Twitternamen und Fotos drauf. Was ist also die richtige Rechtsgrundlage? In so einem Zusammenhang fallen einem zwei Dinge ein, berechtigtes Interesse und Wissenschaft, denn wir untersuchen das und nehmen schon den wissenschaftlichen Hintergrund in Anspruch. Zu unserem Erstaunen haben wir dann festgestellt, dass Artikel 6 (1f) DSGVO die richtige Rechtsgrundlage für uns ist, denn es gibt keine Ausnahme für die For-

schung im Bereich der einfachen Daten. Es gibt eine im Bereich der besonderen Kategorien von Daten, also wenn mit DNA oder mit Gesundheitsdaten geforscht wird, aber eben nicht für ganz einfache Datenverarbeitung. Das ist vermutlich übersehen worden, uns gestern erst aufgefallen, so als spannender Nebeneffekt.

Es ist ja im Datenschutzrecht vieles beim alten geblieben, aber ein Bereich ist neu, nämlich die Verpflichtung, über die Datenverarbeitung zu informieren. Nach der Feststellung der Rechtsgrundlage folgt also die durch die DSGVO neu eingeführte Informationspflicht. Das stellte uns vor die Herausforderung, die Betroffenen bei Erhebung oder kurz danach zu informieren. Wie haben also alle angeschrieben und ihnen mitgeteilt, dass wir ihre Tweets verwenden, wir haben ihnen die Rechtsgrundlage, die Zwecke der Verarbeitung und zuständige Aufsichtsbehörde mitgeteilt.

Die Antworten fielen ganz unterschiedlich aus und waren sehr interessant, denn es waren ja alles ExpertInnen aus der Datenschutzszene. Einige haben einfach nur gelacht, weil die gemerkt haben, dass es im Grunde eine Nachricht mit einem gewissen Augenzwinkern war. Es kann natürlich nicht sein, dass wir hier für zwanzig Tweets stundenlang mit Juratext die Twitter-DMs oder die Impressumsadressen der jeweiligen Blogs verstopfen.

Andere ExpertInnen haben uns tatsächlich ihre Einwilligung mitgeteilt, dabei hatten wir gar nicht um Einverständnis gebeten, sondern nur informiert. Wir mussten ja nicht um Einverständnis bitten, das ist alles gesetzlich gedeckt. Wir hatten nur eine reine Informationspflicht. Anscheinend hatten einige den Unterschied Einwilligung als Rechtsgrundlage und Informationspflicht noch nicht ganz verstanden.

Einige haben sich tatsächlich nur bedankt und dachten, das wäre jetzt ein bisschen Werbung. Da haben wir auch überlegt, das ist eigentlich eine witzige Idee, das eigene Produkt zu bewerben, indem man sagt, wir müssen jetzt leider informieren über unsere Datenverarbeitung mit diesem fantastischen Produkt, das sie bei unserem Datenschutzcompliancemarketingmenschen erwerben können. Wir dachten, eigentlich wäre das eine witzige Idee, Datenschutz als Standortvorteil. Das bringt uns dann auch gleich zum ersten Tweet und der Frage, worum es eigentlich wirklich bei diesem Gebilde Datenschutz/Datenschutzrecht geht.

Worum geht es eigentlich: Schutzgut des Datenschutzes

Im ersten Tweet stellt der Twitternde diese ganz korrekte Frage und sagt, diese könne man nicht beantworten, ohne vorher das Schutzgut im Datenschutzrecht überhaupt zu klären. Es ist im Grunde das erste, was wir nach dem Geltungsbeginn der DSGVO gemerkt haben, dass nach wie vor – eine ewig alte Debatte – völlig unklar ist was eigentlich der Datenschutz ist. Die DSGVO will Artikel 8 der Grundrechte-Charta umsetzen; da steht so was drin wie Recht auf Schutz personenbezogener Daten. Was genau das aber ist, ist weitestgehend ungeklärt. Was machen also die JuristInnen? Die machen das, was sie immer machen, nämlich das, was früher schon gemacht wurde, und das ist besonders in Deutschland, in der deutschen Debatte natürlich das Volkszählungsurteil und die Debatte davor, und wenn man sich genauer anguckt was tatsächlich in der deutschen Diskussion vertreten wurde, merkt man, dass vom Steinmüller-Gutachten bis zum Bundesverfassungsgerichtsurteil sehr früh sehr viel Kritik an dem Ansatz formuliert wurde, das Ganze auf Privatsphäre und Privatleben zu stützen. Aber genau das ist aktuell der Stand in Deutschland, das ist auch bei vielen Experten, die das Thema diskutieren, immer noch in den Köpfen drin. Datenschutz ist Privatsphärenschutz, Datenschutz ist Schutz des Rechts auf Achtung des Privatlebens. Ob das richtig ist, kann kann man bestreiten; wir werden das an vielen Punkten merken, dass das eine falsche Wahrnehmung ist, weil das Recht auf Privatleben tatsächlich Datenschutz reduziert auf Selbstbestimmung – Datenschutz aber ein Grundrecht ist, das sämtliche Freiheitsrechte: Meinungsfreiheit, Versammlungsfreiheit, Asylfreiheit: alle Freiheitsrechte die die Charta oder das Grundgesetz schützen wollen, schützen will. Das heißt, es geht im Grunde darum, den Menschen im Rahmen des digitalen Wandels davor zu schützen, dass er durch die Datenverarbeitung Eingriffe in seine Rechte erlebt, nicht nur sein Recht auf unbeobachtet sein, auf Selbstbestimmung, und wir werden sehen, dass an vielen Stellen dieses alte Denken, dass es immer noch beim Datenschutz nur um Selbstbestimmung und Persönlichkeitsrechte geht, sehr viele Fehlschlüsse produziert. Worum geht es überhaupt beim Datenschutz? Wie weit reicht er eigentlich? Und das ist die nächste Frage: Kann man eigentlich der Datenschutz-Grundverordnung entkommen? Ist das Rechtsgebiet, dass wir betrachten, überhaupt anwendbar?

Sachliche Anwendbarkeit

Da kommen wir dann gleich zu dem ersten Bereich: die sachliche Anwendbarkeit, die Reichweite der Datenverarbeitung, und da gab es eben diese spannende Frage, was ist denn mit den Visitenkarten, die ich auf solchen Veranstaltungen wie hier bekomme und mit nach Hause trage. Gibt es da Informationspflichten, was folgt daraus? Da ist zuerst einmal zu sagen, die Datenschutz-Grundverordnung erfasst ja erst mal nur die automatisierte Datenverarbeitung, und im analogen Bereich das, was veraktet wird, was sortiert wird, also kann man sich erst einmal merken: Visitenkarten, einfach so in der Schublade als großer Haufen ungeordnet: Kein Problem; raus aus dem Anwendungsbereich. In dem Moment, in dem ich das einscanne, sortiere und vielleicht dann auch noch Drittanbietern zur Verfügung stelle, bin ich im Anwendungsbereich der Grundverordnung.

Die andere Frage, die sich immer stellt, ist, wie ist das eigentlich bei personenbezogenen Informationen, wenn die an die Öffentlichkeit gelangen? Das beste Beispiel dafür ist der Aushang der Krankheitstage im Betrieb. Dem Chef stinkt, dass Leute fehlen, und kurzerhand macht er sich kleine Zettel und schreibt darauf, wer alles krank gewesen ist und hängt das in den Flur. Er sagt, das ist zur Information der Mitarbeiter, damit die alle

wissen, wer da ist und wer nicht. Fällt das unter die Grundverordnung oder nicht? Es ist erstmal keine automatisierte Datenverarbeitung, und das ist ein Aspekt, den wir auch in der aufsichtsbehördlichen Praxis immer wieder zu bearbeiten haben. Datenschutz ist kein Geheimnisschutz, darum geht es erst mal nicht. Ausgenommen ist auch der gesamte Bereich der persönlichen Verarbeitung: alles was die Privatsphäre, betrifft, was ich zu Hause für mich mache, was ich nicht teile nach außen, das ist von der Grundverordnung ausgenommen in Artikel 2 und unterfällt der Grundverordnung nicht, aber es gibt natürlich viele Bereiche, in denen vermischt sich dieses private Häusliche: Mit meinem Handy, wenn ich zum Beispiel bei Whatsapp bin und da dann im Hintergrund ein Datenaustausch stattfindet. Was ist, wenn ich twittere? Unterfällt das der DSGVO?

Soziale Medien

Das ist tatsächlich eine der Fragen, die auch in der Szene heiß diskutiert werden: Wenn ich jetzt auf Twitter meine persönliche Meinung äußere, ist es eigentlich etwas, was der Datenschutz-Grundverordnung unterfällt? Das hätte ganz dramatische Folgen, da wäre ich nämlich verantwortlich für das was ich auf Twitter tue: Ich muss meinen Informationspflichten gerecht werden, unter anderem meinen Namen angeben, weil ich ja den Verantwortlichen der Datenverarbeitung benennen muss. Das würde im Umkehrschluss bedeuten, dass wir dank der DSGVO eine Klarnamenpflicht in der Nutzung von sozialen Medien haben. Die Frage ist unbeantwortet, es gibt unter den Aufsichtsbehörden die einen, die selber twittern, die sagen, das sei alles nicht so schlimm, und es gibt die, die das ein bisschen strenger sehen und sagen, eigentlich müsste man, wenn man die ganze Geschichte ernst nimmt, tatsächlich die Nutzung von Twitter darunter fassen, weil es eben eine Datenverarbeitung ist, die immer die Öffentlichkeit betrifft; das ist nichts, was im Privaten bleibt, in einer geschlossenen Nutzergruppe, sondern es ist für alle Öffentlichkeit sichtbar. Da hat der OGH eigentlich ziemlich klar gesagt, wenn es für die Öffentlichkeit sichtbar ist, unterfällt es der Grundverordnung. Das Problem ist im Grunde eines von vielen, wo man merkt: Die DSGVO stellt Anforderungen auf, aber so richtig vollziehen mag man sie doch nicht, weil das zu wahnsinnigen Verzerrungseffekten und im Grunde gesellschaftlich gar nicht hinnehmbaren Folgen führen würde, wenn wir das durchziehen würden, und das ist so ein Motto, dass man an vielen Stellen der Grundverordnung sieht: Wenn man sie ernst nehmen würde, würde sie nicht funktionieren.

Einwilligung

Der nächste Tweet, der so ein bisschen zeigt, wo die Debatte hinläuft, ist einer über eine Aussage von – unter anderem – Jan Albrecht, aber ist nur exemplarisch und das führt fort, was ich anfangs sagte: Die Unklarheit darüber, reden wir hier über Privatsphärenschutz, über Selbstbestimmung, reden wir über Datenschutz oder was ist überhaupt Datenschutz? Ein ganz ganz erheblicher Teil der klassischen Vertreter der Datenschutzszene fokussiert sich unglaublich stark auf die Einwilligung. Da gibt es Begriffe wie „Die Königin der Rechtsgrundlagen", „Kern des Datenschutzes" und „Grundprinzip des Datenschutzes", und das ist eine Aussage, die ist schlicht falsch. Die ist falsch aus zwei Gründen: Es gibt da dogmatische Gründe, da könnten wir jetzt juristisch darüber reden, was genau eigentlich Einwilligung soll. Ist sie eine Beschränkung von einem Grundrecht oder ist es eine Ausübung? Rein dogmatisch passt die Einwilligung überhaupt nicht dazu, dass wir hier von Privatsphäre und allgemeinem Persönlichkeitsrecht reden. Viel wichtiger ist aber, dass die Einwilligung, wenn man sich so sehr auf die Einwilligung fokussiert, zu zwei Dingen führt: Erstens entfaltet sie überhaupt keinen Schutz mehr; ich kann nicht mehr zählen, wie oft ich auf einer Website einfach nur noch blind OK klicke, bei diesen ganzen Cookie-Bannern. Ich soll zu *manage options* gehen und dann kann ich *performance cookies* definieren und *tracking cookies* und *necessary cookies* – kann ich alles machen, oder ich will einfach nur ein Zitat lesen auf der Webseite und sage: Ich nehme dafür nicht 15 Minuten feingranulare Einstellungen vor. Ich willige ein, aber ich willige nicht wirklich ein. Dass ist eine reine Fassade, ist im Grunde nur der Anschein von Rechtmäßigkeit, der nur dazu führt, dass die Einwilligung völlig entwertet wird, weil das für die Menschen keinen Schutz mehr hat, weil die Nutzer einfach nur sagen, ich will meinen Dienst nutzen. Das heißt, wer so sehr auf die Einwilligung fokussiert, entwertet die Einwilligung. Bei Datenverarbeitungen, die massenhaft identisch auftreten wie zum Beispiel im Internet: immer gleiche Sachverhalte, immer wiederholt durch Webseiten-Besucher, ist die Einwilligung überhaupt keine angebrachte Möglichkeit, Datenschutz sinnvoll zu regulieren.

Kopplungsverbot

Das wissen natürlich auch diejenigen, die so ein bisschen sehr sich auf die Einwilligung einstellen, und die versuchen, das dann zu retten mit etwas – das ist jetzt ein juristischer Begriff, der aber vielleicht auch schon mal außerhalb der juristischen Kreise Wellen geschlagen hat: Dem sogenannten „Kopplungsverbot". Das Kopplungsverbot – hier ein sehr schöner Tweet von einer Rechtsanwältin, die sich darüber beschwerte, dass das Kopplungsverbot die Privatautonomie einschränkt – was meint sie damit, erzähle ich gleich, aber das wichtigste, was alle im Saal einfach mitnehmen können: Es gibt in der Datenschutz-Grundverordnung kein Kopplungsverbot. Was ist das Kopplungsverbot? Das Kopplungsverbot ist die Idee, dass, wenn man mehr Datenverarbeitung als für den Vertrag gefordert ist, rechtfertigen will, also der Dienstanbieter mehr erfassen will, als er eigentlich aufgrund der vertraglichen Leistungen an Daten bräuchte, wenn er das über eine Einwilligung rechtfertigen will, dann muss man diese Einwilligung so ein bisschen genauer angucken, ob die freiwillig ist und man damit mehr macht als man eigentlich für den Vertrag braucht. Das ist unter dem Stichwort *Kopplungsverbot* genannt. Ein solches Kopplungsverbot, das dieses verbieten würde, gibt es in der Grundverordnung nicht; es ist nicht verboten, über eine Einwilligung mehr Datenverarbeitung zu rechtfertigen, als man für die Vertragserfüllung braucht. Ganz im Gegenteil: Wenn das

der Fall ist, muss man genauer hingucken, ob die Einwilligung freiwillig ist und was die Praxis daraus macht. Die muss trotzdem noch freiwillig sein, obwohl man sagt: Du kriegst den Dienst nur, wenn du einwilligst. Sie lösen das ganze darüber, dass sie die Einwilligung retten, indem sie sagen, dann biete eine Alternative an, die du bezahlst, wo diese Datenverbindung nicht so intensiv ist – und wozu führt das? Das führt dazu – was wir aktuell und damit im Bereich der Onlinemedien ganz häufig sehen – es gibt jetzt den Basistarif, also quasi wie immer, volles Tracking, aber man braucht ja eigentlich kein Tracking um eine Webseite aufzurufen. Man braucht keine Cookies, um eine Webseite zu lesen. Das ist also nicht wirklich erforderlich, also ist die Einwilligung, was die Freiwilligkeit angeht ein bisschen kritisch. Dann bieten wir eben, um die Freiwilligkeit zu retten – also quasi wieder als Fassade – nebenbei einen Premiumdienst an für alle die nicht getrackt werden wollen, um die Freiwilligkeit der Einwilligung für alle anderen zu erhalten. Das ist die Idee. Für alle anderen, die sagen, ich kann mir das gar nicht leisten, aber die haben ja theoretisch jetzt eine Wahl, und da sie eine Wahl haben, ist es wieder freiwillig. Wozu führt das in der Praxis? 99 % der Leute werden weiter genauso getrackt wie vorher und 0,03 % kaufen sich das Privacy-Add-on, werden damit zu einer datengeschützten Elite und für die anderen ändert sich überhaupt nichts. Das ist im Grunde das Problem, dass das Kopplungsverbot gesamtgesellschaftlich wahnsinnige Verzerrungswirkung haben kann. Das muss man noch mal sehen, wie sich das entwickelt, aber die Idee, den Fokus auf die Einwilligung zu retten über dieses komische Kopplungsverbot, da halte ich überhaupt nichts davon.

Globaler Exportschlager?

Wir haben also in der europäischen und auch in der deutschen Debatte aufgrund eines nicht ganz passenden Grundverständnisses von Datenschutz ein sehr schiefes Verständnis davon, worum es im Kern geht, um Einwilligung, und das schöne ist, das exportieren wir jetzt in die ganze Welt. Die Frage, ist die DSGVO der Exportschlager, der sie vorgibt zu sein? Ist Europa der neue Datenregulierer der ganzen Welt? Hat die Welt auf die DSGVO gewartet? Man kann sagen, die DSGVO hat sozusagen krakenartig ihre Fühler in die Welt herausgestreckt, über den Artikel 3, indem sie bestimmt, dass ein Unternehmen, das Datenverarbeitung auf dem europäischen Markt anbietet, auch wenn es in den USA sitzt, dann der Datenschutz-Grundverordnung unterfällt. Hat das dazu geführt, dass die DSGVO mehr Wirkung entfaltet? Das werden wir sehen, die Unternehmen versuchen sich zum Teil darauf zu fokussieren; wir wissen aus Umfragen, dass nach eigener Einschätzung der Unternehmen ca. 24 % datenschutzkonform agieren. Das ist also noch nicht so rasend viel. Was wir zur Kenntnis nehmen, ist, dass in einigen Drittstaaten es auch Datenschutzregulierung gibt, die sich auch in der Tat an der Grundverordnung orientiert. Das ist aber eigentlich keine Besonderheit, das gab es auch schon zu Zeiten der Richtlinie. Insbesondere im südamerikanischen Raum gibt es eine sehr lebhafte und eine sehr am europäischen Datenschutzrecht orientierte Regulierung.

Kalifornien – das war dann auch groß zu lesen – ist der DSGVO auch ein Stück weit gefolgt und hat einige Aspekte aufgegriffen, ist zum Teil ja aber auch sogar darüber hinausgegangen. Im Asia-Pacific-Raum haben wir immer schon datenschutzrechtliche Regeln gehabt, die sich aber mehr am US-amerikanischen Verständnis von Datenschutz orientiert haben. Da muss man wahrscheinlich auch noch ein bisschen abwarten, wie sich das tatsächlich entwickelt, inwieweit wir tatsächlich aus der DSGVO heraus einen globalen Standard bekommen. Was es aber zu fragen gilt, auch vor dem Hintergrund, dass wir das vielleicht auch politisch exportieren wollen, ist die Frage, was exportieren wir denn da eigentlich? Ist das nur die Einwilligung, ist das so ein diffuses Verständnis von Datensouveränität und was ist dann überhaupt der Gegenstandsbereich? Damit kommen wir dann zu einer der Kernnormen der DSGVO, ohne die genauen Rechtsgrundlagen.

Rechtsgrundlagen – bitte zu Ende lesen …

Die sind alle in einem Artikel geregelt, den müssen wir jetzt nicht nennen, aber das schöne ist, wenn wir die DSGVO zu Ende lesen würden – und das tun tatsächlich einige nicht so gerne – dann würden wir sehen, da stehen nach der Einwilligung noch eine ganze Menge anderer Rechtsgrundlagen. Wir dürfen Daten verarbeiten, wenn wir Verträge erfüllen müssen, wenn sie in unserem Interesse stehen, wenn dies zur öffentlichen Aufgabenerfüllung notwendig ist, es lebenswichtig ist, das ist alles möglich. Die Einwilligung ist eine von vielen Rechtsgrundlagen, wenn man das mit exportieren würde, das wäre zum einen ein Gewinn und da gab es – direkt am 25. Mai – einen mir sehr sehr nachvollziehbaren Tweet: Ich habe zwar selbst kein Auto, aber ich habe ins Lenkrad von meinem Fahrrad gebissen, als ich den halben Tag im Radio gehört habe, die DSGVO habe den Vorteil, dass jetzt BürgerInnen von Behörden und Unternehmen immer um Zustimmung gefragt werden müssen, bevor ihre Daten verarbeitet werden. „Lenkrad zeigt inzwischen Abdrücke meiner Zähne …" Ganz genau so ging es mir auch, das ist längst nicht der Fall, die Einwilligung ist überhaupt nicht der Kern der Grundverordnung, sie ist eine von 6-7 Rechtsgrundlagen, die alle auch geprüft werden müssen. Für Unternehmer ist das auch das Entscheidende: die Empfehlung, dass bitte auch zu tun, denn die Einwilligung ist jederzeit widerrufbar. Wenn wir ein Geschäft aufbauen und uns nur auf die Einwilligung verlassen, dann kann, wenn wir einen Datenschutzskandal haben, mal eben die Einwilligung für den Abo-Dienst widerrufen werden, und dann kann das ganze Geschäftsmodell in sich zusammenfallen, weil wir auf die Einwilligung gesetzt haben und dank dem Widerruf die ganze Datenverarbeitung ihre Rechtsgrundlage verliert. Deswegen in jedem Fall die Empfehlung: Bevor man sich auf die Einwilligung als Ultima Ratio verlässt: alle möglichen Rechtsgrundlagen prüfen: Vertragserfüllung, berechtigte Interessen, alles was man finden kann, um hier nicht am Ende auf einmal den Teppich unter den Füßen weggezogen zu bekommen.

Und eine ganz andere Frage: Was ist denn nun, wenn man sich auf die Einwilligung verlassen hat, zum Beispiel: Ich bin eine große Supermarktkette und sage, ich hätte gern Kundenkartenprogramme, und alle die wir hier sitzen, sagen, alles klar 3 % Rabatt bei jedem Einkauf, das mache ich mit, und macht es über eine Einwilligung. Irgendwann ist mein Geschäft vielleicht in Verruf und Sie sagen, ich widerrufe diese Einwilligung. Und dann sage ich: Moment mal, das hätte ich auch im Vertrag schreiben können, ich switche mal um auf eine andere Rechtsgrundlage. Und das ist im Grunde das Problem, dann ist nämlich die Folge, wenn man nicht vorher die Grundverordnung zu Ende liest, wenn man sich einmal auf die Einwilligung eingelassen hat, dann suggeriert man

ja so eine Art Gleichordnung und so eine Ebene, wo quasi zwei gleichrangige Parteien sich das so überlegt haben, wenn die dann sagen, da nehme ich mal wieder die Rechtsgrundlage, die im Gesetz steht, Vertragserfüllung, dann – vielleicht nicht herrschende Ansicht aber eine sehr starke Ansicht bei den Juristen – da ist der Rückgriff gesperrt, dann haben sie Pech. Dann ist die Einwilligung weg und etwas anders können Sie nicht nehmen. Deswegen ganz klare Empfehlung: In der Grundverordnung immer zu Ende lesen und sich nicht immer gleich auf die Einwilligung zu stürzen.

Soft Law oder harte Regulierung?

Der nächste Tweet betrifft Artikel 5, was bietet die DSGVO eigentlich noch als Rechtsgrundlage? Wir haben eine ganze Reihe von Regeln, und eine der Kernregelungen in der DSGVO ist Artikel 5, das sind die Grundsätze der Datenverarbeitung. Nun gibt es diesen Streit, wie verbindlich sind die eigentlich? Ist das eigentlich nur Gesetzgebungsprosa oder ist das auch verbindlich? Muss man das umsetzen, Soft Law oder Regulierung? Die DSGVO ist eindeutig mehr als Einwilligung, das haben wir gehört, mehr als Rechtsgrundlagen die Programmsätze, die Grundsätze werden in Absatz 1 beschrieben. Interessant für uns ist aber auch der Absatz 2, der häufig auch nicht mehr mitgelesen wird. Im Absatz 2 wird nämlich die Verantwortlichkeit festgeschrieben, und das ist auch deutlich stärker herausgearbeitet worden in der Grundverordnung im Vergleich zur Richtlinie: Dass die Verantwortlichen, sei es ein Unternehmen für sich oder gemeinsam mit anderen Unternehmen, oder auch eingebundene Auftragsverarbeiter rechenschaftspflichtig sind, und insofern wird der Artikel 5 Absatz 2 meines Erachtens etwas unterschätzt. Der sagt nämlich, der Verantwortliche muss nachweisen, dass er mit den Regelungen der Grundverordnung compliant ist. Daraus folgt der Anspruch, dass der Verantwortliche verpflichtet ist, Prüftransparenz herzustellen, und Prüftransparenz ist sozusagen die Baustelle im Datenschutzrecht und in der Datenschutzumsetzung. Jedenfalls aus aufsichtsbehördlicher Sicht und aus Sicht der Durchsetzung von Datenschutzrecht, weil ich Datenschutzrecht nur durchsetzen kann, wenn ich es auch prüfe, und ich kann es nur prüfen, wenn in den Unternehmen die Datenverarbeitung auf eine Art und Weise gestaltet ist, die prüffähig ist. Wenn ich erst in ein Unternehmen komme und da ist alles kuddelmuddel, dann fange ich erst mal an zu sortieren und dann komme ich vielleicht am fünften oder sechsten Prüftag erst zur eigentlichen Prüfung. Die Grundverordnung verpflichtet jetzt die Unternehmen, ihre Datenverarbeitung so aufzubereiten, so transparent zu machen, so zu dokumentieren, dass sie prüffähig ist, und davon ausgehend folgen eine ganze Menge Pflichten. Unter anderem auch die Transparenzpflicht,

Durchsichtige Transparenz

Und da sind wir schon wieder bei meinem Lieblingsthema am heutigen Tag. Die Transparenz ist ein ganz erheblicher Teil, der die Grundverordnung prägt, und das sieht man auch an vielen Tweets und das spiegelt so ein bisschen den Geist wider, in dem wir in der ganzen Debatte leben. Transparenz ist im Grunde die Supermaßnahme, Transparenz ist quasi die Lösung für alles, und das ist genauso ein Problem, wenn man auf die Selbstbestimmung, Privatleben schaut, die Einwilligung fokussiert, dass Transparenz im Grunde zum Selbstzweck hochstilisiert wird. Und das ist tatsächlich etwas, was ich auch extrem kritisch sehe, aus dem einfachen Grund, dass Transparenz alleine keinen Wert hat. Wenn wir zum Supermarkt gehen und sagen, ich hätte gern einen Liter Milch und gehen dann zum Regal gucken und gucken uns an, was auf einem Liter Milch steht. Dann ist auf der Milch gedruckt, Achtung, enthält Arsen, ist supergiftig, nicht kaufen – ja, super transparent. Ich will aber nicht im Supermarkt eine halbe Stunde verbringen, das Kleingedruckte zu lesen, um zu gucken, welche Milch giftig ist. Transparenz alleine hat überhaupt keinen Wert. Wenn wir Artikel 8 DSGVO, Recht auf Schutz personenbezogener Daten ernst nehmen, dann müssen wir aus Transparenz immer auch irgendeinen Schutz ableiten, und das bedeutet schlicht, das es, genauso wie im Lebensmittelrecht üblich, höchste Vorgaben dafür gibt, dass man keine Milch mit Arsen verkaufen darf. Und das ist genau die Folgerung, die man, wenn man Transparenz isoliert betrachtet, vergisst: Es klingt manchmal so, als müsste man nur ins Kleingedruckte genug reinschreiben und den Nutzern klar machen, was alles an Unfug getrieben wird, Dann ist doch alles gut, dann ist es transparent. Klar, wenn man nur auf Selbstbestimmung abstellt, dann ist Transparenz der Inbegriff von Datenschutz, aber ich will eben nicht nur die Möglichkeit haben, zu wissen, was ich mir schlechtes antue – ich will schlicht davor geschützt werden. Das heißt, Transparenz ist in weiten Teilen tatsächlich auch ein Buzzword der DSGVO, und Buzzword ist genau das nächste Thema, davon gibt es noch eine ganze Reihe mehr in der Datenschutz-Grundverordnung. Vorher noch ein Tweet von Tim Wu, großartiger Professor an der Columbia University of Law, auf den Punkt gebracht: Transparenz ist im Grunde immer nur ein Ersatz dafür, überhaupt etwas zu tun. Aber das ist schwierig, wir müssen irgendwie den Onlinemarkt regulieren, mit so vielen Stakeholdern, und die Werbemenschen machen uns das Leben schwer: einfach Transparenz drauf klatschen, das hilft dann schon, und das ist genau das was der Grundverordnung auch nicht gerecht wird. Transparenz als Master ist im Grunde erst mal nur die Ausrede dafür, sich überhaupt Gedanken zu machen.

Buzzwords by Design

Wir bleiben beim Buzzword. Transparenz ist auch ein Buzzword aber natürlich: Transparenz ist notwendige Bedingung, es ist nur nicht hinreichend, und das Problem haben wir eben bei vielen Dingen in der Grundverordnung. Der Artikel, der das am schönsten zusammenfasst, ist der Artikel 25, der wird bei ganz vielen ganz hoch gelobt, da geht es nämlich um *Privacy by Design*. Das ist im Moment das Number-One-Buzzword neben den jetzt aufkommenden Ethics. Was steht eigentlich hinter dem Artikel 25? Der ist aufgeteilt in zwei Absätze. Der erste Absatz regelt Privacy by Design, der zweite Absatz regelt Privacy by Default. Ich möchte jetzt erstmal ausdrücklich nur über den Absatz

1 reden, der Absatz 2 hat nämlich durchaus einen eigenen Regelungsgehalt. Den würde ich dem Absatz 1 absprechen. Privacy by Design ist eigentlich nichts anderes als eine sehr wirkungsvolle, sehr mundgerechte, sehr marketingtechnisch gut gemachte Zusammenfassung dessen, was die DSGVO eigentlich will. Sie möchte, dass ich, bevor ich in eine Datenverarbeitung eintrete, also bevor ich anfange, automatisierte Datenverarbeitung zu betreiben – die fällt ja nicht vom Himmel, die muss ja designed werden, ich muss mir mal Gedanken machen, was für Daten will ich denn überhaupt verarbeiten, ich brauche auf jeden Fall immer Hardware und ich brauche immer Prozesse die das regulieren. Ich muss mir am Anfang eigentlich immer Gedanken machen, und das möchte Artikel 25 zum Ausdruck bringen: Mach Dir vorher Gedanken, bevor du in eine Datenverarbeitung einsteigst, und darüber hinaus mach Dir nicht nur Gedanken, sondern denk auch daran, dass es Rechtsvorschriften gibt, die Dir sagen, was du darfst und was du nicht darfst, und beachte die. Das ist nämlich ein Punkt den man erwähnen muss, der scheinbar nicht bekannt ist, dass es durchaus Rechtsbereiche gibt, die reguliert sind, und dass man sich dann tunlichst auch an die Vorgaben hält. Die Vorgaben mögen nicht immer präzise sein, manchmal sind sie genereller Natur, aber nichtsdestotrotz muss man sie beachten. Um das zu institutionalisieren, diesen Vorgang des Vorher-Gedanken-Machens, gibt es in der Grundverordnung eine Regelung, die sehr sinnvoll ist, und das ist das Datenschutz-Impact-Assessment. Das ist wirklich auch eine Neuerung der DSGVO, das gab es vorher so nicht in der Richtlinie, und das ist ein echter Mehrwert. Kleiner Haken an der Sache: Das Datenschutz-Impact-Assessment ist nur für Datenverarbeitung mit einem besonders hohen Risiko gesetzlich vorgegeben, das ist ein bisschen misslich, ist aber auch nicht so schlimm, weil man ja vorher zu dem Ergebnis kommen muss, dass für die Datenverarbeitung, die ich plane, kein hohes Risiko besteht. Wie komme ich dazu? Das sagt die Grundverordnung nicht explizit. Was ich aber immer empfehlen würde, und da kommen wir dann vielleicht auch zu den positiven Seiten der DSGVO, da kann nämlich ein echter Mehrwert daraus entstehen: Bei jeder Datenverarbeitung, bei jedem Projekt erst mal so ein Mini-Assessment zu machen; sich also die Daten anzugucken, die verarbeitet werden, die Software, die Hardware, die Prozesse, die Personen, die ich einbinde, und dann eine Risikoabschätzung zu machen: In welchem Bereich unterliege ich rechtlichen Vorgaben, in welchem nicht, wie tief ist die Eingriffsintensität? Das hat mehrere Vorteile: Einmal: Ich weiß ungefähr, dass ich mich rechtlich auf sicherem Terrain bewege, ist also ein Aspekt des Risikomanagement. Der andere Aspekt ist, dass ich im Idealfall tatsächlich weiß, was ich tue. Das ist vielleicht für so kleine EntwicklerInnen oder kleine Start-ups nicht so das Problem. Je größer das Unternehmen aber wird, desto schwieriger wird es, genau diese Frage in den Griff zu bekommen. Ich habe unterschiedliche Entwicklungsabteilungen, die alle vor sich hin arbeiten, und irgendwann wird das zusammengeführt. Aber wenn es dann zusammengeführt wird, weiß eigentlich niemand mehr so richtig, was da eigentlich passiert. Ich brauche immer jemanden, der den Überblick behält, und wenn man so ein Datenschutz-Impact-Assessment macht, Privacy by Design ernst nimmt, dann kommt da hinterher etwas heraus, das vernünftig dokumentiert ist, das sich dann jemand anschauen und diesen etwas weiteren Blick über die Datenverarbeitung behalten kann. Das wäre dann eine Win-Win-Situation.

Verarbeitungsverzeichnis – Bürokratie oder Empowerment?

Wir haben in der Grundverordnung noch eine weitere Regelung, die, wenn man sie ein bisschen intelligent anwendet, durchaus zu so einer Win-Win-Situation führen kann, und zwar ist das die Vorschrift, dass Verarbeitungsverzeichnisse zu führen sind. Da könnte man jetzt sagen, was ist das denn für eine blöde Bürokratie? Hat das auch noch andere Folgen, ist das Bürokratie oder Empowerment? Ich würde sagen, wenn man das intelligent macht, dann kann das dazu führen, dass ich tatsächlich Kontrolle über meine Verarbeitungstätigkeiten erlangen kann. Das Management muss sich nämlich fragen, was tue ich eigentlich? Welche Daten verarbeite ich eigentlich? Das führt immer wieder zu überraschenden Ergebnissen, wir haben das bei uns in der Dienststelle zum Beispiel auch gemacht, und dann kam heraus, dass wir mehr Verfahren haben, als wir eigentlich selbst dachten. Es ist immer wieder ein spannender Prozess, der am Ende dazu führt, dass ich weiß, was ich was ich tue. Der insofern – und so kann man das dem Management auch immer sehr gut verkaufen – ein Aspekt des Risikomanagement ist. Ich kann mich ja nur schützen vor Risiken, wenn ich sie überhaupt kenne, und insofern kann ich eigentlich nur empfehlen, dieses Verzeichnis der Verarbeitungstätigkeiten ernst zu nehmen und durchaus kleinteilig zu betreiben und nicht zu grobgranular. Wenn ich das grobgranular mache, dann hat es wirklich keinen Mehrwert für das Unternehmen, dann ist es wirklich nur Bürokratie. Wenn ich das aber ein bisschen feingranularer mache, dann tauchen da manchmal Dinge auf über die ich selbst überrascht bin.

IT-Sicherheit: falsche Schwerpunktsetzung ...

Für mich persönlich die wichtigste Regelung in der Grundverordnung, eine die sich ein wenig versteckt. Was wir jetzt häufig erleben, ist, dass gerade bei den externen Datenschutzbeauftragten oder auch bei den betrieblichen Datenschutzbeauftragten der Fokus sehr stark auf die IT-Sicherheit gelegt wird. Wie hängen IT-Sicherheit und Datenschutz eigentlich zusammen? In der Grundverordnung geregelt wird die Sicherheit der Verarbeitung in Artikel 32, eine der Normen, die ich mit zu den vier bis fünf wichtigsten Normen der Grundverordnung zählen würde. Neben Artikeln 4, 5, 6 ist das der Artikel 32. Warum? Artikel 32 muss in dem Kontext der Grundverordnung gelesen werden, das heißt, er betrachtet eben nicht nur die klassischen IT-Sicherheitsziele, also Vertraulichkeit, Verfügbarkeit und Integrität, sondern geht darüber hinaus. Der Artikel 5 spielt eine große Rolle, und was was der eigentliche Kern ist: Über Artikel 32 kommt das Recht oder fließt das Recht in die Technik ein. Das ist nämlich genau die Schnittstelle, die wir brauchen, um rechtliche Anforderungen in die Technik zu überführen, und das machen wir in der Regel mit Schutzzielen und mit den daraus generierten Maßnahmen. Die sollen sicherstellen, dass das, was wir rechtlich vorgeben, auch tatsächlich in der Technik ankommt. Jetzt haben wir – und das sehen wir ganz deutlich gerade in Artikel 5 und Artikel 32 –, dass da Schutzziele, Maßnahmen, Grundsätze wild durcheinander gewürfelt sind. Das liegt vermutlich daran, dass die Grundordnung in erster Linie von Lobbyisten, zumindest aber von Juristen gemacht worden ist. Einige Väter und Mütter der Grundverordnung waren halt Juristen und insofern ist dieser Bereich dann einfach ein bisschen zu kurz gekommen – auch vor dem Hintergrund,

dass die Grundverordnung natürlich den Anspruch hat, technikneutral zu sein. Aber Technikneutralität heißt ja nicht, dass man keine Vorgaben macht, die man auch technisch umsetzen kann. Insofern würde ich sagen, Artikel 32 ist ausbaufähig. Maßnahmen sind eigentlich die der Umsetzung der Grundverordnung.

Transparenz ist für die anderen …

Ich habe ja schon ein bisschen frech über die Transparenz geschimpft, und wollte nur einen Punkt noch betonen, denn witzigerweise verlangt die Grundverordnung von den Aufsichtsbehörden etwas Neues, nämlich dass sie Transparenz wahren bei der Besetzung ihrer Spitzenposten. Das ist eine positive Entwicklung der Grundverordnung, dass erstmals wir zumindest eine Vorgabe haben, bei der Besetzung der Spitzenposten: klare Vorgaben, Bestenauslese, orientiert an dem Vorbild für den europäischen Datenschutzbeauftragten, kompliziertes Auswahlverfahren, Ausschreibung. Das Problem ist bisher, obwohl die Grundverordnung gilt, dass alle Posten, die bisher besetzt worden sind oder die dabei sind, besetzt zu werden, das scheinbar ignorieren, d.h. wir könnten jedenfalls nicht feststellen, ob die Personen, die dann wirklich benannt werden, auch die bestgeeigneten sind.

Who watches the Watchmen?

Wir wissen es schlicht nicht, weil wir keinen konkreten Vergleich haben, und wozu das führt, kann am besten daran messen, wie sich die Aufsichtsbehörden gerade zumindest so schlagen. Wenn man sich das mal anguckt, dann findet man unter anderem das Problem, dass die Aufsichtsbehörden – die 18, die wir haben, also jedes Bundesland eine, Bayern zwei und der Bund – sich alle gerne mal widersprechen, sich in die Quere kommen, und das ist etwas, wo man fragen muss: Funktioniert es eigentlich gerade mit der Grundverordnung?

Endlich mit Biss?

Und wenn man dann eine Aussage wie diese liest, dass der hessische Datenschutzbeauftragte sagt, bisher waren wir zahnlos und jetzt haben wir Zähne bekommen; wir sind zwar nicht bissig, aber wir haben Biss – das ist etwas, da kann ich mich einfach nur wundern, denn entweder hat Herr Ronellenfitsch die vorherige Rechtslage nicht richtig verstanden und seine eigenen Befugnisse nicht gekannt, dann schon vorher gab es die Möglichkeit, Bußgelder bis 300.000 € zu verhängen. Das wurde nie ausgenutzt, also die Bußgelder sind nie an diese Grenze gekommen, und es war nie so, dass die Datenschutzbeauftragten sagten, wir hätten gerne, aber wir konnten nicht mehr. Oder er hat tatsächlich die Grundwerte und die neuen Kompetenzen falsch eingeschätzt, und was aus dieser komischen Gemengelage jetzt entsteht, ist eine ganz merkwürdige Situation von Unsicherheit und von einer Drohkulisse, die den letzten Punkt, den ich vielleicht noch anspreche, nämlich das berühmte Blogsterben betreffen.

Bußgelder und Blogsterben

Es scheint bei den Nutzern auf einmal die Sorge zu sein: Jetzt kommt auf einmal die Grundverordnung und macht mir den Blog dicht, weil ich ein Komma in der Datenschutzerklärung falsch gesetzt habe. Das ist genau dieser verschobene Blick, der aus dieser Betonung kommt, jetzt haben wir richtig Macht bekommen, jetzt haben wir wirklich Eingriffsbefugnisse bekommen, die tatsächlich aber im wesentlichen vorher schon bestanden. Warum sie jetzt auf einmal mehr vollzogen werden dürfen, wissen wir nicht, werden wir sehen. Das Problem ist, dass diese Drohkulisse, die aufgebaut wird, mit Forderungen, wie auch zum Beispiel jetzt endlich 4 % des Jahreseinkommens auch zu vollstrecken, diese Drohkulisse kann sich auch zum Bumerang entwickeln. Wenn wir in fünf, sechs Monaten merken, da kommt nichts, dann wird das möglicherweise eine kleine Blase, dann wird man vielleicht das Problem haben, dass uns auch keiner mehr ernstnimmt. Da muss man sehen, wie diese neue Drohkulisse nachher umgesetzt wird, ob tatsächlich die Grundverordnung hier zu einem besseren Vollzug führt oder nur zu viel Sorge – und dann ist auch nichts draus geworden.

Goldstandard?

Bleiben wir bei der Frage: Ist denn die Grundverordnung jetzt der neue Goldstandard? Damit ist 2012 mal Viviane Reding angetreten: Die Grundverordnung sollte Goldstandard sein. Lassen wir mal die Frage offen.

Kirsten Bock und Malte Engeler

Kirsten Bock ist Juristin und arbeitet seit 2004 im *Unabhängigen Landeszentrum für Datenschutz*. Dort hat sie das Europäische Datenschutz-Gütesiegel, kurz *EuroPriSe*, gegründet. Derzeit arbeitet sie zusammen mit Martin Rost und anderen an der Entwicklung des Standard-Datenschutzmodells, einem systematischen und Grundrechte-fokussierten Verfahren zum Datenschutzmanagement. Sie ist Mitglied der Grünen.

Malte Engeler ist promovierter Rechtswissenschaftler, aktuell Richter am Schleswig-Holsteinischen Verwaltungsgericht. Zuvor hat er vier Jahre im Bereich der nationalen und europäischen Datenschutzaufsicht gewirkt und kennt die DSGVO gut. In seinem Blog *deathmetalmods* kommentiert er kritisch vor allem Hardware und Dienstleistungen.

FIfF e. V. – Stefan Hügel

Weizenbaum-Studienpreis 2018 – Einleitung

Liebe Mitglieder des FIfF,
liebe Freundinnen und Freunde,
liebe Gäste,
liebe Preisträger des Weizenbaum-Studienpreises 2018,

seit diesem Jahr widmen wir unseren Studienpreis – und die später noch zu vergebende Medaille – Professor Dr. Joseph Weizenbaum, der die Gründung des FIfF gefördert hat, dem wir 1998 einen Ehrenpreis des FIfF für seinen Einsatz für Verantwortung in der Informatik verliehen haben und der dessen langjähriges Vorstandsmitglied war.

Bereits im letzten Jahr habe ich ihn mit Worten zitiert, die ich so treffend finde, dass ich sie heute wiederholen möchte. Über sich selbst hat er einmal gesagt:

> *„Ich bin kein Computerkritiker. Dieser Begriff ist sinnlos. Computer können mit Kritik nichts anfangen. Nein, ich bin Gesellschaftskritiker. Es geht mir um die Rolle des Computers in unserer Gesellschaft."*

In Gedenken an Joseph Weizenbaum, der vor nunmehr zehneinhalb Jahren verstorben ist, verleiht das FIfF heute seinen Studienpreis 2018.

Auch unsere diesjährige Konfrenz zeigt es wieder deutlich: Informatiksysteme sind geronnene Machtstrukturen, die dafür genutzt werden, die Produktivität der menschlichen Arbeitskraft zu erhöhen und ihre Nutzung zu optimieren – Karl Marx hätte wohl gesagt: zur Erhöhung des Mehrwerts im Interesse des Kapitals. Bei ihrer Konzeption und Implementierung werden Entscheidungen getroffen, die diese Machtstrukturen festlegen und weiter verfestigen. Dies gilt für alle Bereiche: Für die industrielle Produktion, für Dienstleistungen, für das Militär, für die öffentliche Sicherheit. Funktionierende Technik wird stets auch angewendet – unabhängig von ihrer Rechtmäßigkeit und ihrer Sozialverträglichkeit.

Es ist die gesellschaftliche Aufgabe der Informatikerinnen und Informatiker, technische Systeme auch von ihren ethischen, sozialen und rechtsstaatlichen Anforderungen her zu denken, um eine Technik zu verhindern, die zum Selbstzweck wird und schädliche Nutzung als „Sachzwang" etabliert. Mit unserem Studienpreis wollen wir Arbeiten auszeichnen, die dieser Aufgabe gerecht werden.

Wir bedanken uns herzlich für die große Zahl an Arbeiten, die in diesem Jahr bei uns eingereicht wurde. Eine Jury, besetzt mit

- Professorin Britta Schinzel aus Freiburg,
- Professorin Marie-Theres Tinnefeld aus München, die uns zu juristischen Aspekten beraten hat,
- Professor Jochen Koubek aus Bayreuth,
- Rainer Rehak aus Berlin,
- René Malsky aus Münster,
- und mir selbst, Stefan Hügel aus Frankfurt am Main

hat aus den Einreichungen für den Studienpreis 2018 vier Arbeiten ausgewählt, die wir heute hier prämieren werden.

FIfF e. V. – Rainer Rehak: Laudatio für den 1. Preis

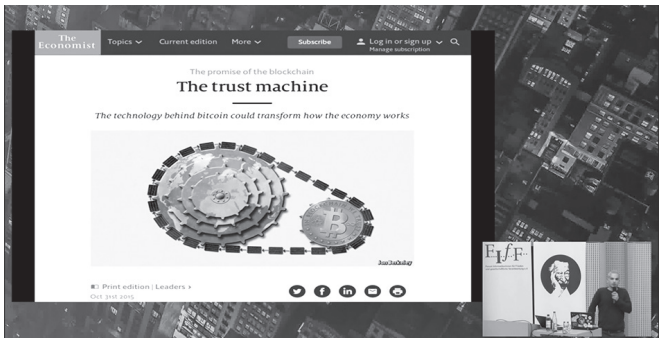
Leon Kaiser: Vulnerable Systems. The Quantification of Affect in an Experimental Blockchain Pilot-Project for Financial Transactions Management for Refugees

Bachelorarbeit an der Leuphana-Universität Lüneburg

Es ist mir eine große Freude und Ehre, jetzt den ersten Platz des Weizenbaum-Studienpreises zu annoncieren und zu übergeben. Und zwar haben wir ihn vergeben an eine Bachelorarbeit, angefertigt an der Leuphana-Universität Lüneburg, an der Fakultät für Kulturwissenschaften, Institut für Kulturästhetik digitaler Medien. Und zwar trägt sie den Titel: *Vulnerable Systems. The Quantification of Affect in an Experimental Blockchain Pilot-Project for Financial Transactions Management for Refugees*.

Erst einmal ein schöner langer Titel, mit ganz vielen Labels, die gerade herumfliegen, allerdings bewegt sich diese Arbeit von Leon Kaiser nicht in der kassisch-affirmativen Jubelposition, wie sich doch durch den Einsatz von Blockchain die Welt zum

Laudator Rainer Rehak



Folien aus der Präsentation, Übergabe des Preises (unten)

Besseren wenden lässt, sondern wirft einen ganz konkreten Blick auf ein existierendes Blockchain-Projekt und analysiert an dieser Stelle, inwiefern weniger die technischen Eigenschaften der Blockchain selber, sondern inwiefern die Versprechungen der Blockchain in diesem konkreten Projekt umgesetzt wurden, oder wie es das beeinflusst hat. Das heißt an der Stelle, es behandelt hauptsächlich den Diskurs, aber immer auch mit Rückgriff auf die technischen Grundlagen.

Das große Thema ist dabei das Vertrauen in die Blockchain, das heißt eine Eigenschaft, die einer Technologie zugeschrieben wird, wobei gerade das Vertrauen eine bestimmte, ja eine besondere Aura hat – dazu werden wir gleich noch mehr hören – und es ist an der Stelle interessant, weil es wie so oft in Technik-Diskussionen nicht über das *Jetzt* geht, sondern über die *Zukunft*, d. h. die Versprechungen beziehen sich natürlich immer auf eine Zukunft, die durch Einsatz von Technik eine bessere Zukunft ist.

Erst wird die Blockchain-Technologie vorgestellt, und dann geht es um die Ankündigungen, Versprechungen und Anwendungsfälle, die proklamiert werden, und dann geht es um das *World Food Program* von den Vereinten Nationen, und wie da digitale Identitäten durch Blockchain dargestellt werden sollen. Das heißt, das Thema ist eigentlich Techno-Utopismus – wenn man es so nennen möchte – und das Thema sind die Zuschreibungen an Technik und die damit verknüpften Entscheidungen. Wie wir ja hier die ganze Zeit auch sehen und lernen, hängen natürlich die Folgen von Techniknutzung oder die Fragen in bezug auf Technikeinsatz davon ab, wie darüber gedacht wird und nicht, wie die Eigenschaften tatsächlich sind.

Interessant dabei, ich will nur ein paar Punkte nennen, die für das FIfF insbesondere relevant waren für die Auszeichnung dieser Arbeit von Leon Kaiser – ansonsten hören wir ja gleich noch etwas –, war zum Beispiel, inwiefern das Vertrauen in die Blockchain genutzt werden sollte, um sie in Vertrauen für das World Food Program zu übersetzen, d. h., dass die *Vulnerable Groups*, also denen da geholfen wird, nicht alleiniges Ziel sind, sondern auch eine Rechtfertigung, z. B. den Geldgebern gegenüber – wo man schon einmal merkt, in welchem Bereich so eine Technik Wirkung entfalten kann.

Was man, wie so oft, bei – proklamierten – Einsatzmöglichkeiten der Blockchain erkennt, ist ein Vertrauen, das in Code proklamiert wird, und nicht mehr in Institutionen, wobei ganz klar herausgestellt wird, dass Verwundbarkeiten, die dadurch vielleicht reduziert werden, an anderer Stelle noch viel schlimmer, oder vielleicht in anderer Form, wieder aufkommen, und die Bedeutungsverschiebung oder die Deutung des Vertrauens dann in so einer Art *Algorithmic Authority* oder *Trust by Computation* – daran merkt man, wie diese Technikzuschreibungen dann auch versuchen, aus diesen komplexen, unverstehbaren Bereichen der sozialen und institutionell organisationalen Interaktionen auszubrechen, dass man die dann verschieben kann auf Technik und Algorithmen, denen vertraut wird, und wir als Technikbewegte – wenn man diesen Begriff verwenden will – wissen natürlich, dass das in größten Teilen auf ähnlichem Terrain gebaut ist, wie das blinde Vertrauen in soziale Interaktionen und Organisationen.

Im Ergebnis zeigt sich ein Zitat, das Lawrence Lessig neulich geäußert hat: „The young people always innovate oblivious to the past", also es sieht so aus, als würde die Jugend immer Innovationen vorantreiben und dabei komplett die Vergangenheit vergessen. Die Vergangenheit zu vergessen heißt an der Stelle, nicht zu erkennen, dass bestimmte Diskussionen schon einmal geführt worden sind und beantwortet; dass bestimmte Probleme schon einmal aufgekommen sind, und dass es bestimmte Eigenschaften gibt, die komplexer zu verstehen sind, als auf den ersten Blick zu erkennen ist.

Wir haben diese Arbeit ausgezeichnet – damit möchte ich schließen – weil sie nicht in einem allgemeinen *Für-Blockchain* oder einem allgemeinen *Gegen-Blockchain* bestand, sondern auf eine ganz konkrete Anwendung geblickt hat und diese sehr interessant analysiert hat mit sehr kreativen Denkweisen, und damit erkenntnisfördernd sowohl für Leute aus der Informatik als auch für Leute, die nicht Informatik betreiben, aber dennoch sich für diese Themen interessieren.

Leon Kaiser, ich bitte Dich auf die Bühne für die Übergabe – Herzlichen Glückwunsch.

Severin Engelmann: The Digital Dimensions of Personal Identity

Masterarbeit an der Technischen Universität München

Der Vorfall um Cambridge Analytica ist noch immer in aller Munde. Offenbar waren Daten von 87 Millionen Nutzern betroffen. Wenn man diese Zahl relativ zu den aktiven Facebook-Nutzern (2 Milliarden) sieht, sind dies freilich gerade einmal 4%.

Facebook aber hat Zugriff auf 100% der Daten, was genau macht Facebook eigentlich damit? Richtig, Sie betreiben Microtargeting und schalten maßgeschneiderte Werbung. Gerade wurde bekannt, dass selbst Telefonnummern, die NutzerInnen angeblich aus Sicherheitsgründen bereitstellen sollten, für diesen Zweck genutzt werden.

Und wie wirkt sich das wiederum auf die Nutzer und die reale Welt aus?

Damit beschäftigt sie die Arbeit unseres Preisträgers *Severin Engelmann*, dessen Arbeit *The Digital Dimensions of Personal Identity* wir heute mit dem Weizenbaum-Studienpreis auszeichnen. Die Arbeit ist am Munich Center for Technology in Society an der Technischen Universität München erstellt worden.

Die Arbeit untersucht den Einfluss der Sozialen Medien – in diesem Fall der Plattform Facebook – auf die Konzepte persönlicher Identität. Fünf philosophische Identitätstheorien werden dafür zunächst untersucht:

- John Locke – Erinnerungskriterium
- Dan Zahavi – Experimentelles Selbst
- Mariya Schechtman – Narrative Selbstkonstitution
- Harry Frankfurt – Willenskraft zweiter Ordnung
- Charles Taylor – Schwacher und starker Evaluator

Der Autor analysiert dann das User Interface für die EndnutzerInnen und die Werbeschnittstelle – Facebook nennt es: Audience Targeting Application – des sozialen Netzwerkes. Er zeigt dabei den Zusammenhang zwischen der realen Welt sowie die abstrakte Abbildung der Realität in die Benutzerschnittstelle von Facebook. Ebenso stellt er die Abbildung der Benutzerschnittstelle in die Marketingschnittstelle dar.

In seiner Schlussfolgerung stellt der Autor zunächst den Zusammenhang zwischen drei Ebenen dar: Der realen Welt, der Abbildung der realen Welt in die Benutzerschnittstelle von Facebook und der Abbildung der Benutzerschnittstelle in die Marketingschnittstelle von Facebook. Die Transformation geht in beide Richtungen: Auch die Marketingschnittstelle beeinflusst die Benutzerschnittstelle, und diese wiederum die reale Welt. Damit sind alle Facebook-Nutzer weltweit an dem Modell der sozialen Welt beteiligt, das von den Entwicklern von Facebook vorgegeben wird. Die Werbung wird durch weitere Feedback-Schleifen optimiert.

Wir zeichnen diese Arbeit mit dem Weizenbaum-Studienpreis aus, da sie ein besseres Verständnis über soziale Netzwerke und ihrer Funktionsweise schafft. Die Analyse der Benutzer- sowie Marketingschnittstelle und dessen Wirkung zurück in die reale Gesellschaft zeigt, wie einerseits die Marketingkonzepte von sozialen Medien durch die Öffentlichkeit beeinflusst werden und wie die öffentliche Meinung umgekehrt durch Microtargeting beeinflusst werden kann.

Die Arbeit wendet philosophische Konzepte auf ein aktuelles Phänomen der realen Welt – der Kommunikation und Interaktion über soziale Netzwerke – an und schafft dadurch die Grundlage für ein besseres Verständnis dieser sozialen Netzwerke und ihrer Funktionsweise. Die Analyse der Marketing- und Benutzerschnittstelle und der Rückwirkung dieser Schnittstellen auf die reale Gesellschaft schafft ein Verständnis dafür, wie einerseits die Marketingkonzepte von sozialen Medien durch die Öffentlichkeit beeinflusst werden, und wie die öffentliche Meinung umgekehrt durch Microtargeting beeinflusst werden kann. Dazu werden in kreativer Weise die Erkenntnisse der Philosphie zur menschlichen Identität herangezogen. Die Jury hat sich einhellig für die Auszeichnung der Arbeit entschieden.

Herzlichen Glückwunsch, Severin Engelmann, zum Weizenbaum-Studienpreis 2018.

Folie aus der Präsentation (oben), Übergabe des Preises

Severin Engelmann

The Digital Dimensions of Personal Identity. An Analysis of Facebook's User Interface and Audience Targeting Application

2. Preis

Personal identity is a multidimensional construct subjected to various influences that are intricately difficult to define. Before the intellectual turning point of The Enlightenment in 18th century Europe, religious dogma largely determined the fundamental aspects of personal identity: every person was first and foremost a child of God. Importantly, dogmatic conceptualizations of personal identity were stable principles and hardly ever revised. Beyond the dogmas of religion, however, individuals always had some freedom of self-comprehension. Such a hermeneutical dimension of personal identity comprises the possibilities that enable individuals to form intelligible self-concepts within a communal, cultural, and historical meaning giving structure. Thus, the hermeneutical dimension of personal identity describes how individuals apply meaning to the diversity of experiences in the context of culturally pre-defined concepts. For example, cultural rituals and traditions provided narrative self-conceptions for individuals independent of the influential principles of religious dogma.

With the philosophical ideas of The Enlightenment authority over the normative and descriptive nature of personal identity began to slowly transform to the intellectual world of the individual human being. Today, we know that humans are biological organisms consisting of a set of different units called cells that all share a similar genetic makeup. Thus, natural sciences represent another significant dimension of personal identity as a construct.

Personal identity is subjected to dogmatic influences today: in law, personal identity is standardized in constitutions. For example, the Basic Law for the Federal Republic of Germany approved in 1949 specifies in article 1, sentence 1: "Human dignity is inviolable".[1] While human dignity should not be conflated with personal identity, this example nonetheless demonstrates that legal texts enshrine the legal dimensions of personal identity. Moreover, such legal standards are usually less malleable: article 1, sentence 1 cannot be altered or modified in any way, as it is an eternity clause that persists as long as the German constitution is in effect.

Overall, while the religious and legally specified dimension of personal identity are relatively stable, the scientific and, in particular, hermeneutical dimension of personal identity are more dynamic.

1. Modeling the Social World in a Profitable Program

Programmers create mini worlds, i. e., models M of the scope of the reality a program incorporates. In so doing, programmers will need to abstract from the nature of the real world W. In computer sciences, abstraction is a process of imperfect translation: no program is large enough to include all objects of even the tiniest scope of W, the real world. Overall, the interpretation $I: W \rightarrow M$ denotes that I maps W into M: the interpretation of the real world W is represented in a model M. M thereby contains the terms of the objects of the interpretation of W (Figure 1). It follows that if the function $f_M: M \rightarrow M$ denotes any relation between two terms in M, then there is an according function $f_W: W \rightarrow W$ denoting a relation in W so that:

Relations between objects in M have their correspondence in the reality of the world W. In creating a program, a model is a relative concept. The model of a mini world can in turn be interpreted and used as the reality for another model, which involves further abstraction.

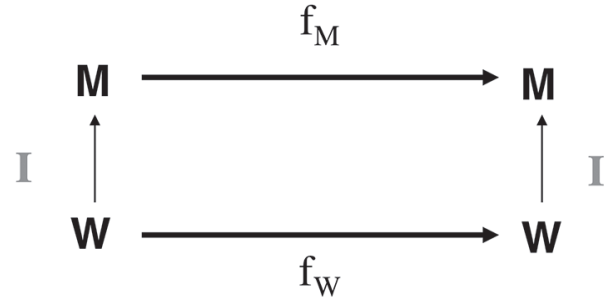


Figure 1: a computer model of a scope of reality in the real world. Relations between objects in M have their correspondence in the reality of the world W.

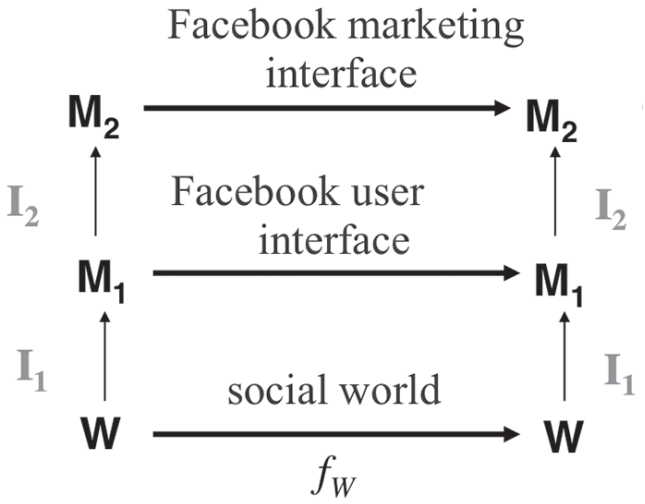


Figure 2: The model M1 ("Facebook user interface") of a scope of reality W ("social world") serves as the basis for M2 ("Facebook marketing interface")

Importantly, this is the case with Facebook (Figure 2). The user interface serves as a model for a subsequent model, the marketing interface. Likewise, any relationship between objects in the user interface will have a correspondent relationship in the marketing interface. However, in the case of Facebook, the concept of a model is somewhat misleading: while a model is often asso-

ciated with a mere simulation of events, the Facebook model of the social world participatory so that:

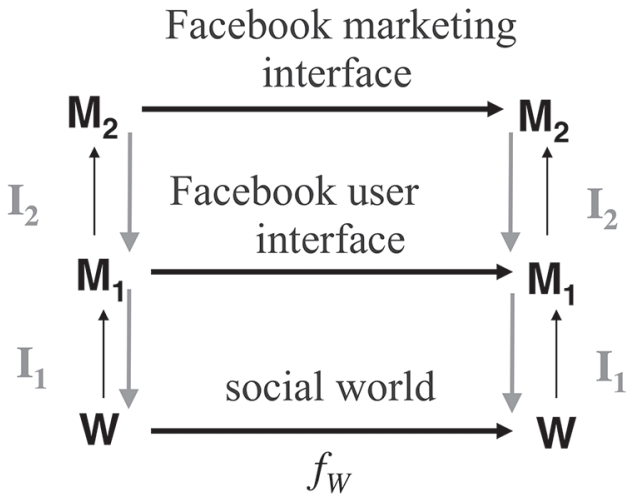


Figure 3: The two models of the social world M1 and M2 are participatory and therefore influence a scope of the social reality W.

To generate monetary value, every action in the user interface has a corresponding economic value in the marketing interface. As such, the user interface represents a system that is fully determined in terms of actions that can be made. The marketing interface is fully determined in terms of the inferences that are made from these actions. The model of the user interface serves a participatory platform for advertisers to influence the user interface, which subsequently influences the social world (see Figure 3, red arrows). Taken together, all Facebook users worldwide participate in an interactive model of the social world as conceived by Facebook's programmers.

The first programmers of Facebook faced the thorny task of modeling a scope of the social world. They had to create a model containing objects such as individuals, interactions, communities, social actions and so on based on their observation and description of the offline social world. Indeed, this demonstrates that creating a digital program purposed to model the social world is inevitably a normative undertaking.

2. People-based Marketing

The following case study will give a glimpse into the possibilities of creating highly specific audiences for advertising on Facebook. Fundamentally, there are two different approaches: first, advertisers themselves put together the target audience. Second, advertisers can instruct Facebook to create an audience based on characteristics similar to an existing audience. Such an audience is called a lookalike audience.

2.1 Custom Audiences

Advertisers can provide Facebook with a range of metadata on their customers, such as first and last name, phone number or email address (Figure 4).

Figure 4: when creating a custom audience advertisers upload data of existing customers based on a variety of attributes to directly target on Facebook. https://www.facebook.com/ads/manager/

Once a customer audience has been defined by uploading offline customer data to Facebook, an advertiser can add further filters to that user group by Facebook's audience insights.

Advertisers then target users on Facebook based on demographics, interests, and behaviors. Figure 5 reveals the large variety of people-based marketing options offered to advertisers by Facebook.

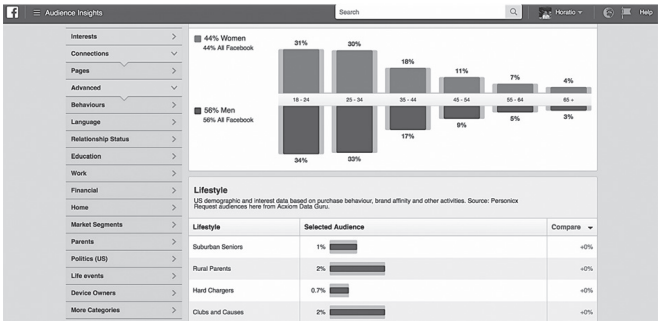


Figure 5: left column indicates the vast range of categories by which advertisers can target users on Facebook in addition to metadata. https://www.facebook.com/ads/audience-insights/

A relatively specific audience on Facebook could include the following filters: as an advertiser, I might wish to target females who have recently been in Manhattan in New York City, but are no longer there; are between ages 20 and 30; speak English and match the criteria "new parents" or "Mums: new Moms" or "Parents (01 – 02 years)", "Parents with Toddlers" or "expectant parents" who also are interested in "eBook readers".[2] Figure 6 shows the final audience in Facebook's Adverts Manager.

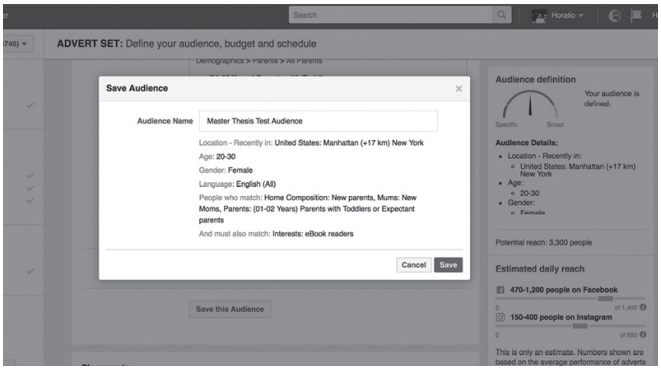


Figure 6: an audience created with Facebook's "Audience Insights" tool. https://www.facebook.com/ads/audience-insights/

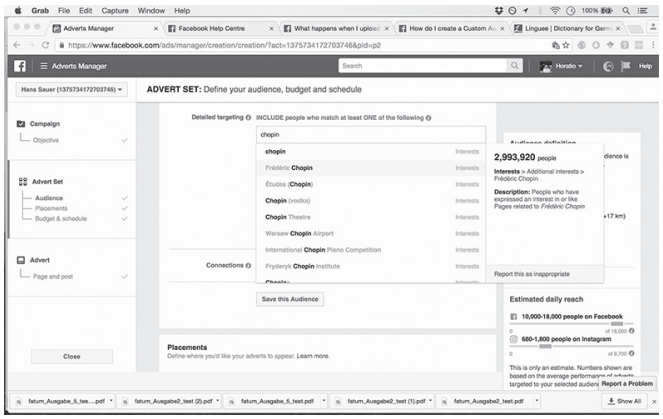


Figure 7: targeting options for an audience to which Facebook assigns the interest "chopin" on Facebook's "Audience Insights". https://www.facebook.com/ads/manager/

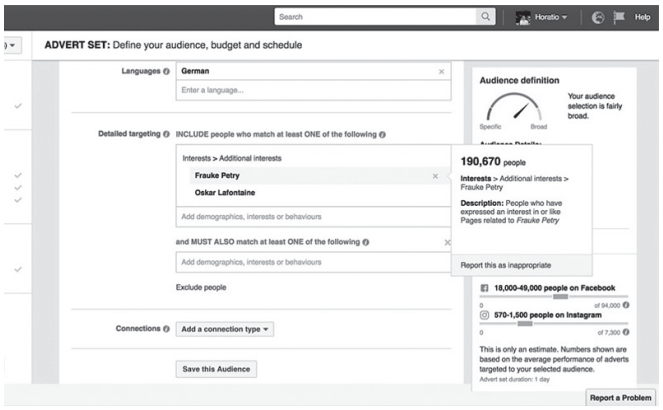


Figure 8: targeting users with an "Interest" in two German politicians from opposite camps: Frauke Petry and Oskar Lafontaine. https://www.facebook.com/ads/manager/

In the previous example, a relatively specific audience was created and shown. Filters work like search engines for human characteristics. Audiences can be selected according to almost any interest or behavior one can think of. Figures 7 and 8 display how users' interests and behaviors can be retrieved in Facebook's Audience Insights tool. The first search query targets users with the "Interest" in the musical composer Frederic Chopin, while the second attempts to target users with the "Interest" in two German political figures from opposite camps: the ultra-conservative, right-wing Frauke Petry from the "Alternative Für Deutschland" party as well as the left-wing Oskar Lafontaine, member of "Die Linke" party.

2.2 Lookalike Audiences

An alternative strategy for targeting users on Facebook is setting up a so-called lookalike audience. Generally, a lookalike audience consists of users that Facebook evaluates as "similar" in preferences, interests, behaviors, gender, age, location (and others) to users that already share a connection with a fan page, a business, or a website on Facebook (i.e. that have already been profiled). Figure 9 below shows the set-up of such a lookalike audience within the Audience Insights tool in the Facebook marketing interface.

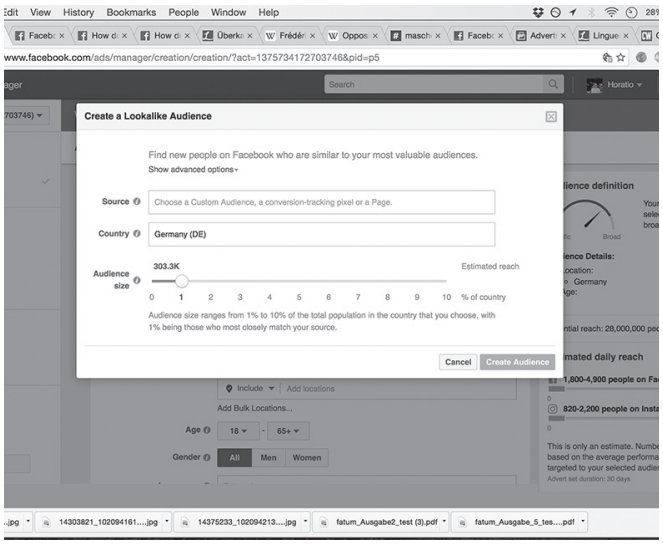


Figure 9: creating a lookalike audience. https://www.facebook.com/ads/manager/

With this introduction to Facebook marketing, we can now turn to our original analysis of three philosophical theories of personal identity to understand how these relate to Facebook's digital social realism.

3. Facebook and two Philosophical Theories of Personal Identity

3.1 Maya Schechtman's Narrative Self-Constitution View

Schechtman's theory of personal identity consists of two central elements: first, personal identity is a matter of self-interpretation, which, second, is subjected to different external influences, in particular, the interactions with others.[3]

According to Schechtman, personal identity is a life-long process whereby a person constitutes herself by organizing her experiences into a linear narrative. Life consists of experiences, however, only some are actually attentively perceived, interpreted and acted on. Meaning is given only to a handful of these experiences. A person emerges if she carries out "…the psychological work required to organize these experiences in an ongoing, self-reflexive narrative".[4] Additionally, a person comes to realize the boundaries of her person in terms of her story's uniqueness: other individuals have different stories.

But what is the nature of a person's narrative? First of all, a person's narrative depends on self-interpretation: an individual compares and relates experiences and organizes them by certain culturally-determined standards in order to constantly attribute meaning to the large amount of events that she experiences every day. It follows that no time-slice – any momentary event that an individual experiences – is in any way definitive for a person's identity. Only when interpreted in the context of the narrative, is such a time-slice a descriptive and meaningful element of a person.[5] Second, such narrative contexts are necessary for individuals in a social environment. A person's choices and actions must be"…flowing intelligibly from …(his)… inten-

tions, motives, passions, and purposes, that is…tell a narrative that explains it.[6] Without our narrative context, other individuals cannot make sense of our choices and actions.

The formation of a meaningful and consistent interpretation of one's self is fundamentally linguistic.[7] Schechtman's narrative account tries to demonstrate that the life of human beings is not simply a biological process, but a continuous and coherent linguistic articulation that individuals form. It is the capacity to psychologically organize a stream of events in a culturally accepted form of a narrative "…by which we will come to think of ourselves as persisting individuals with a single life story."[8] The narrative view gives individuals freedom to shape who they wish to be, re-interpret their past self-image, and anticipate their future self. Additionally, other individuals are potentially significant partakers in creating or changing an individual's narrative. Thereby, personal identity is essentially procedural as well as actively negotiated between subjective and objective narrative accounts of a person.

The marketing system of Facebook does not only collect, process, and evaluate what users willingly present of themselves on Facebook. The inferences data analysis techniques draw from the activities of a user generate a parallel narrative, which we will term formalized narrative: there is the person's own narrative, the narrative others have of that person as well as a formalized narrative made by technological systems – in this case Facebook. The system's interpretation of a person is fed back to the person by advertisement. It is therefore reasonable to say that Facebook generates a formalized narrative made for economic purposes.

The custom audience shown in Figure 6 illustrates that one data type, in this case location, can be combined with how users present themselves, who their friends are or how much time they spent on certain fan pages and so on.

One could therefore argue that with Facebook use, personal identity is subjected to a completely new form of narrative – one that is generated by formalized principles that infer information about individuals they are completely unaware of and cannot engage with. Today, a person, his or her social network (offline and online), and Facebook all participate in creating a person's narrative.

3.2 Facebook and Harry Frankfurt's Second Order Volition

In his essay "Freedom of the Will and Concept of a Person"[9], Harry Frankfurt (*1929) develops a notion of personal identity grounded in the structure of human will. Thereby, humans are capable of deciding what desire they wish to be moved by when desiring some action.[10] A person can think and care about the desirability of its desires. Frankfurt calls such desires "second-order desires", which are desires about desires, or wants about wants. Non-human animals have desires or urges, for example, eating or sleeping. Frankfurt calls the desire to eat and the desire to sleep "first-order desires". Animals have no authority over whether they want to have these desires or not – they have no capacity to determine any reasons to act on a desire other than the impulse or urge manifested in that desire.[11] It follows that the object of a first-order desire is a state of affair while a second-order desire's state of affair is having or not having a first-order desire.

Humans can be vegetarian, for example: a person can want to want to eat in a certain way – here, vegetarianism, an ethical principle, governs how she acts on her desires. The problem is that a person could have multiple second-order desires at once without making any of them the underlying principle for action.

Participating in Facebook (posting self-relevant information), the second-order desire to receive positive feedback from others is highly likely to be the effective and most prominent desire and will therefore represent the majority of users' second-order volition. Social influence is incorporated into the technological set-up of Facebook – also on the marketing side, for example through lookalike audiences. This is perhaps best illustrated by looking at the initial setting-up phase of a profile. Take, for example, two Facebook profiles. One of the two profiles is completely new on Facebook with no friends and no information provided, while the other one has been on Facebook for a couple of years. The new profile will be called "Newbie", the established profile will be termed "Oldie".[12] Figure 10 shows the news feed of Newbie that contains no information or posts by others or any advertisement (names are crossed out for privacy protection).

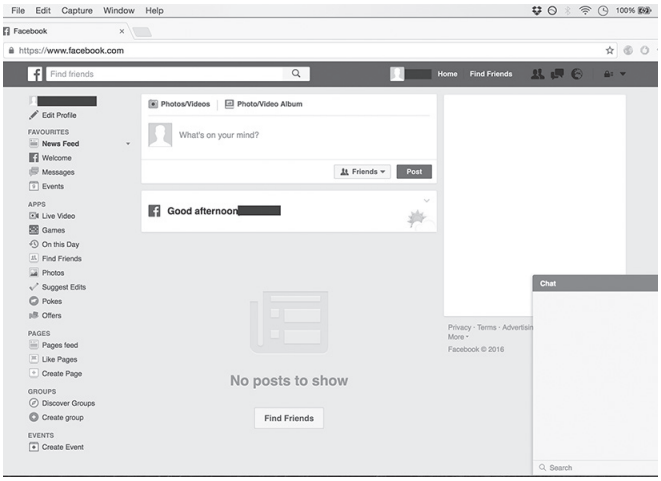


Figure 10: Newbie's empty news feed. https://www.facebook.com/

What happens, however, if Newbie and Oldie become friends? Figure 11 below indicates how Newbie's news feed changes directly after accepting a friendship request from Oldie (Newbie now has one friend on Facebook: Oldie).

Facebook fills Newbie's news feed with information related entirely to Oldie's profile. Figure 12 illustrates how Facebook adjusts Newbie's informational space with Oldie's social affiliations as well as preferences and interests.

For example, the news feed now presents a post of one of Oldie's friends (who isn't friends with Newbie) that Oldie interacted with (see center red rectangle "liked this") and suggests Newbie to send a friendship request to that profile (see center-right circle "Add Friend"). Moreover, Facebook now suggests pages ("Philosophy Matters") and groups ("Dr. Sebi Recipes") to Newbie, some of which Oldie has interacted with (see "sug-

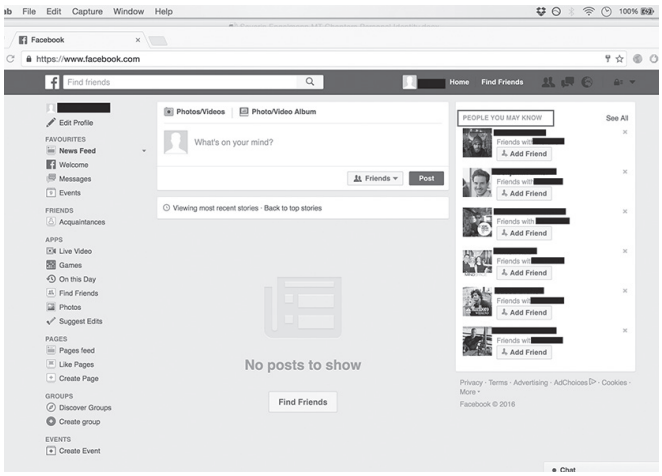


Figure 11: after connecting with Oldie, Facebook instantly proposes a selection of Oldie's social connections to Newbie (see red rectangle). Facebook assumes overlapping social groups for both users. Names are crossed out for privacy protection. https://www.facebook.com/

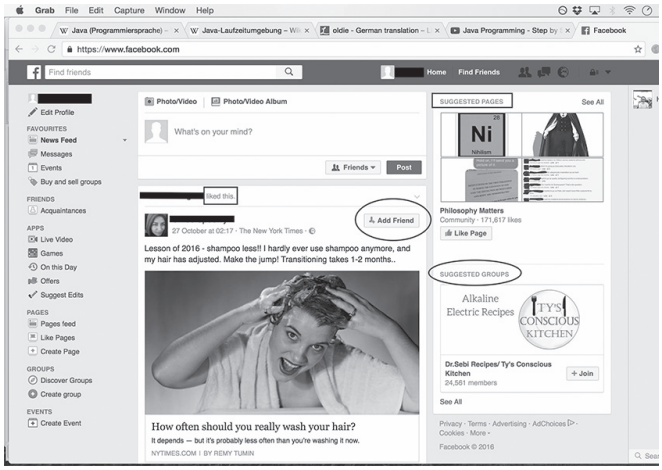


Figure 12: Newbie logging in to Facebook again after becoming friends with Oldie. Red circles and rectangles highlight social as well as advertising posts related to Oldie, now presented in Newbie's news feed. https://www.facebook.com/

gested pages" and "suggested groups").

This small experiment shows how Facebook's user interface nudges individuals to align their self-presentation in a way that is similar to other users. By becoming affiliated with just one other profile, Facebook appears to draw various inferences about a user and, accordingly, provides several calls to action, for example, becoming friends with certain individuals, expressing an interest or joining a group: none of which a user actively expressed as his or her self-evaluation. Thus, targeting the right person is a matter of interpretation carried out by the program: In the real social world, one may come to develop a preference for something because a friend has a preference for that very same thing – a product, a political attitude, or hobby.

Self-presentation is a process that involves second-order desire reflection. However, in the user and marketing interface, self-presentation is heavily inspired, nudged, and technologically staged by the normative element of judging the desirability of one's desires as equal or at least similar to the desirability of other individuals' desires.

4. Summary of Analysis & Conclusion

Frankfurt developed his theory of personal exclusively from the perspective of the individual. On Facebook, and probably social media in general, humans will use reflection for a limited scope of purposes. The value of activity on Facebook is pre-determined: positive evaluation by a social community largely consisting of weak ties. If this is the overall goal of participation, deliberating about the desirability of my desires is, again, pointless, as others will, in the end, provide the significant evaluation of the desirability of my desires – not me. The awareness of myself is dominated by the awareness of how others view me. The philosopher, Luciano Floridi, (*1964) has termed this "digital gaze": the view I have of myself and the view others have of me necessarily converge on such digital social platforms exactly because I can explicitly view how others view me: a phenomenon that does not exist in the offline world.[13]

Such convergence between communication and evaluation is technologically conditioned. A like does not articulate any reasons for approval. However, the person receiving a like from another user will project some intention into his or her evaluation. While a user may have reasons to like another user's post, it is the technological system that actually arranges and orchestrates such procedures. The post is presented to a user as a result of the system making an algorithm-determined decision. Personal identity is embedded in such technologically staged environments today. Frankfurt demonstrates how important the process of reflecting about one's own values and ideals is for personal identity. By turning immaterial human characteristics into explicit economic value, social media essentially determines the nature of these human characteristics for a global society today. Therefore, Facebook is a perfect example of what Mainzer referred to as situational and personalized interaction models built to represent the contents of human consciousness.[14]

Severin Engelmann

Severin Engelmann ...

Facebook's user interface serves as a platform for narrative production, albeit a narrative lacking variety. The differences to narratives created in the offline world lie in the aforementioned attributes of the technological environment: its unique spatial, temporal, and communicative dimensions. The more data my formalized narrative contains, the more rigid and stable it gets – Facebook marketing enhances those attitudes and preferences the formalized data narrative assigns to my profile. In turn, the more I am confronted with my formalized narrative by advertisement the more powerful its self-fulfilling prophecy – perhaps a reason for users to obfuscate. Schechtman's narrative-constitution view helps us understand that today there is a technological narrator in the background. The pressure to conform to the formalized narrative, on the other hand, can be very real for individuals.

The goal of this work was to clarify and understand some of the digital dimensions of personal identity by analyzing Facebook's user and marketing interface. We presented philosophical theories of the hermeneutical dimension of personal identity. Such theories seek to underline and clarify the possibilities and limits of self-comprehension for individuals. Evidently, programmers already program the digital dimensions of personal identity – and will do so in the future.

Anmerkungen

1 https://www.bundestag.de/gg
2 Generally, Facebook enables many audience filters based on life events (such as being pregnant, moving house or moving to another city, or being in a relationship).
3 Schechtman, Marya, The Constitution of Selves, New York: Cornell University Press, 1996, page 95
4 Schechtman, Marya, The Constitution of Selves, page 125
5 Schechtman, Marya, The Constitution of Selves, page 127
6 Gallagher, Shaun, The Oxford handbook of the self, Oxford: Oxford University Press, 2011, page 396
7 Gallagher, Shaun, The Oxford handbook of the self, page 395
8 Gallagher, Shaun, The Oxford handbook of the self, page 399
9 Frankfurt, Harry, Freedom of the Will and the Concept of a Person, The Journal of Philosophy, 68.1, 1971
10 Frankfurt, Harry, Freedom of the Will and the Concept of a Person, page 6
11 Frankfurt, Harry, Freedom of the Will and the Concept of a Person, page 6
12 One author created a new Facebook profile (Newbie) and befriended it with his own Facebook profile (Oldie).
13 Floridi, Luciano, The ethics of information, New York: Oxford University Press, 2013, page 223
14 Mainzer, Klaus, Computerphilosophie zur Einführung, page 173

FIfF e. V. – Stefan Hügel: Laudatio für den 3. Preis

Nico Lück: Künstliche Intelligenz und Rüstungskontrolle. Der Einsatz maschinellen Lernens in Waffensystemen und Verifikationsmaßnahmen

Masterarbeit an der Goethe-Universität Frankfurt am Main

Bereits im letzten Jahr haben wir eine Arbeit ausgezeichnet, die die Anwendung der künstlichen Intelligenz zum Thema hatte – die Anwendung statistischer Klassifikation in der Kriminalprognostik. Seither scheint der Hype um die „Künstliche Intelligenz" den um das Thema „Algorithmen" abzulösen.

Gerade hat der Deutsche Bundestag eine Enquête-Kommission zur Künstlichen Intelligenz eingerichtet. Dass die Beschäftigung mit KI schon lange nicht mehr auf die Informatik begrenzt werden kann, dafür ist die Arbeit *Künstliche Intelligenz und Rüstungskontrolle. Der Einsatz maschinellen Lernens in Waffensystemen und Verifikationsmaßnahmen* von *Nico Lück* ein Beispiel. Sie ist am Institut für Politikwissenschaft der Goethe-Universität Frankfurt am Main entstanden und steht inhaltlich im Zentrum der Aktivitäten des FIfF: Der Einsatz informatischer Methoden in Waffensystemen und in der Rüstungskontrolle. Sie geht, so der Autor selbst, „der Frage nach, welche Folgen der Einsatz lernender Künstlicher Intelligenz … in Waffensystemen und Verifikationsmaßnahmen aus der Perspektive der Rüstungskontrolltheorie hat." Wir zeichnen die Arbeit heute mit dem Weizenbaum-Studienpreis aus.

KI und autonome Waffensysteme können zur Destabilisierung führen, indem sie – anders als Menschen – keinen deeskalierenden Charakter haben, technologisches Wettrüsten fördern und sich die Technologie unkontrolliert verbreiten kann. Sie entzieht sich vielen traditionellen Methoden zur Überwachung und Beschränkung. Die Ansatzpunkte der traditionellen Rüstungskontrolle – eindeutige Materialisierung, Fähigkeiten oder Funktionsweise – scheitern an den intransparenten Eigenschaften von KI: weder nachträgliche Erklärung noch eine vorherige Determinierung der Handlungen sind möglich, da das erlernte Modell nicht einsehbar und damit nicht überprüfbar ist. Es bleibt lediglich die Kontrolle und Beschränkung während des Entwicklungsprozesses oder des aktiven Einsatzes in militärischen Operationen, die eine vertragliche Kontrolle nach traditioneller Logik erschweren. Zudem sind heutige, digitale Innovationen leichter zu kopieren als frühere – mechanische – Innovationen in Waffensystemen, weshalb technologisch überlegene Staaten immer mit sich selbst im Rüstungswettlauf stehen. Weshalb die KI selbst, und nicht die Waffen oder die Waffen in Verbindung mit KI im Fokus der Kontrolle stehen müssen.

Umgekehrt können nach Ansicht des Autors KI-Verifikationsmaßnahmen aus der Perspektive der Rüstungskontrolltheorie die Stabilität unterstützen, indem sie die technische Überwachung seines Erachtens nach zu einer weitaus präziseren und umfangreicheren Informationsverarbeitung befähige und die öffentliche Zugänglichkeit der KI-Methoden für ein intensiveres Engagement zivilgesellschaftlicher Akteure ermögliche.

Letzteres ist kritisch zu hinterfragen, denn mit der Methodenkenntnis ist in der KI keinerlei Ergebniskontrolle impliziert. Bei

den Anwendungsgebieten Satellitenbildinterpretation oder nukleare Überwachung durch Sensorabtastung von Rüstungsgütern und Spektralanalyse von radioaktiven Substanzen könnten KI-Methoden nützlich sein; ebenso bei der Integration diverser Informationsträger mit Geo- und Open-Source-Daten. Die vom Autor für die Zukunft als essentiell geforderten Aspekte um das Vertrauen in die Technologie zu stärken – Transparenz, Kausalität statt Korrelation und Manipulationsschutz –, können jedoch aus unserer Sicht allgemein nicht erfüllt werden, da die Ergebnisse lernender KI-Technologie nicht nur – wie der Autor richtig schreibt – intransparent sind, sondern grundsätzlich kontingente unvorhersehbare, nicht reproduzierbare Ergebnisse liefern. Diese Eigenschaften sind den Methoden inhärent. Ausnahmen können Neuronale Netze, wie für deep learning verwendet, etwa für das Go-Spiel, Schach oder Roboter in abgeschlossenen Bereichen wie am Laufband, bilden.

Nico Lück gibt einen umfassenden Überblick über die Einsatzgebiete der Künstlichen Intelligenz für Waffensysteme und Abrüstungsverifikation und wendet die Rüstungskontrolltheorie überzeugend auf seinen Gegenstand an. Obwohl keine Informatik-Arbeit, ist sie informatisch gut fundiert. Die Verbindung zwischen den politisch-psychisch-sozialen Handlungsspektren und technischen Gegebenheiten gelingt ausgezeichnet. Sie vergleicht auch die US-, russischen und chinesischen Konzepte und Vorgehensweisen; und verknüpft dies alles mit einschlägigen vertraglichen Vereinbarungen. Die Jury hat sich einhellig für die Auszeichnung der Arbeit entschieden.

Herzlichen Glückwunsch, Nico Lück, zum We baum-Studienpreis 2018.

Nico Lück

3. Preis

Künstliche Intelligenz in Waffensystemen als Herausforderung für die Rüstungskontrolle

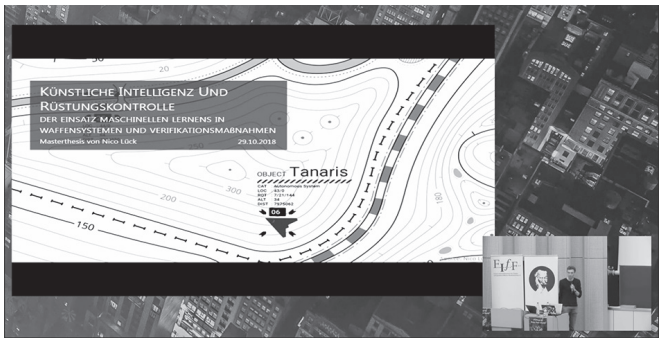
Hinweis: *Dieser Beitrag ist eine stark gekürzte Fassung der Masterarbeit des Autors. Eine ausführliche Fassung mit umfangreichen Literaturkorpus findet sich als eine diesjährige Veröffentlichung durch das Leibniz-Institut Hessische Stiftung Friedens- und Konfliktforschung oder als hinterlegte Masterarbeit an der Goethe-Universität Frankfurt.*

Bei zunehmender Rechenleistung birgt Künstliche Intelligenz (KI) ein großes militärisches Potential. Als rüstungstechnologische Innovation streben Regierungen durch den Einsatz von KI in Waffensystemen eine technologische Überlegenheit und damit einen strategischen Vorteil gegenüber anderen Staaten an. Für die Rüstungskontrolle stellt dieser Umstand ein Risiko dar.

Das Risiko zeigt sich in Waffensystemen, in denen KI absichtlich mit zerstörerischen Aufgaben beauftragt werden kann oder eigenständig einen zerstörerischen Weg zu einem vordefinierten Ziel wählt. Um dieses Risiko zu minimieren, steht Rüstungskontrolle vor der Herausforderung, den Einsatz von KI in Waffensystemen gänzlich zu verbieten. Doch KI entzieht sich den herkömmlichen Ansatzpunkten traditioneller Rüstungskontrolle und minimiert gleichzeitig einen wichtigen deeskalierenden Faktor auf dem Schlachtfeld: die Langsamkeit des Menschen.

Künstliche Intelligenz und maschinelles Lernen

Der Begriff KI ist wegen seiner unpräzisen und tautologischen Definitionen umstritten. Doch für den Zweck dieses Artikels reicht eine Annährung: Die meisten Definition nennen übereinstimmend zwei Kerneigenschaften (1) die Lösung hoch komplexer Aufgaben und (2) die Anpassungsfähigkeit gegenüber der Umwelt. Besonders die Fähigkeit zu Lernen ermöglicht besonders gute Leistungen in diesen Eigenschaften. Denn in der Vergangenheit interpretierten Computerprogramme Sachverhalte anhand von ProgrammiererInnen vorgegebener Regeln. Das sogenannte maschinelle Lernen ermöglicht dem Programm hingegen, selbstständig Regeln auf Grundlage der erkannten Muster in Datensätzen zu generieren. Damit können Programme die komplexe Wirklichkeit besser abbilden und sind nicht von vorgegebenen Lösungswegen abhängig. Die dem Menschen überlegene Leistungsfähigkeit gilt jedoch bisher nur für KI, die für spezifische Anwendungen konstruiert wurde (*narrow AI* oder *weak AI*). Eine generell intelligente Maschine, welche den Menschen als Vorbild hat, existiert bisher und wahrscheinlich für die nächsten Jahrzehnte nicht. Dementsprechend geht es in diesem Artikel um die Folgen von anwendungsspezifischer lernender KI für die Rüstungskontrolle. Durch diese Spezifizierung des Begriffs werden herkömmliche Computerprogramm sowie futuristische KI-Konzepte ausgeschlossen.



Ziele und Maßnahmen der Rüstungskontrolle

Die neusten Entwicklungen im Bereich KI treffen die Rüstungskontrolle in Krisenzeiten: Militär-technologischer Fortschritt, Vertragsbrüche und fehlender politischer Willen lassen das Vertrauen in das multilaterale Instrument sinken. Doch Vertrauen ist ein wichtiger Faktor in einem internationalen System, in der Nationalstaaten immanenten Sicherheitsdilemmata gegenüberstehen: Was schreckt ab? Wie viel ist ausreichend? Was passiert, wenn meine Abschreckung fehlschlägt? Eine Antwort für Re-

gierungen ist es, rüstungstechnologische Innovation zu nutzen, um eine technologische Überlegenheit und damit einen strategischen Vorteil gegenüber anderen Staaten zu erlangen oder auszugleichen. Doch damit dies in keinen Rüstungswettlauf eskaliert, schwächt die Rüstungskontrolle diese Dilemmata, indem sie militärische Kapazitäten und Potentiale reguliert. Diese Regulierungen können auf das Rüstungsvolumen, die geographische Stationierung, den Bereitschaftsgrad oder auch die Nichtverbreitung, Abrüstung oder Abschaffung gewisser Waffenkategorien zielen. Die Ziele der Rüstungskontrolle und der nationalen Militärstrategie sollten damit dieselben sein: Einem gewaltsamen Konflikt ausweichen und eine grundlegende Abschreckung und Sicherheit gewährleisten.

Eine globale Bedeutung erreichte die Rüstungskontrolle erst in der zweiten Hälfte des 19. Jahrhunderts mit dem humanitären Völkerrecht, welches zunächst den Umgang mit Verwundeten, Kriegsgefangenen und der Zivilbevölkerung im gegnerischen Land regelte. Die zahlreichen bi- und multilaterale Rüstungskontrollverträge des 20. Jahrhunderts zeigen, dass konventionelle Waffen, Massenvernichtungswaffen oder selbst die Trägersysteme von Waffen beschränkt wurden und immer noch werden. KI würde sich als Software erstmals in diese Liste einreihen.

Das Kernelement moderner Waffensysteme

Wie bei allen IT-Systemen findet sich auch bei Waffensystemen eine Trennung zwischen Hard- und Software. Zwar verbessern Entwicklungen an der Hardware die physischen Handlungsfähigkeiten und die Feuerkraft von Waffensystemen, doch ist das Entwicklungspotential schlicht durch die Physik begrenzt. Die Verbesserung der Software hat hingegen noch erheblich höheres Potential, da es keine natürlichen Grenzen im Agieren in einer komplexen Umwelt und Reagieren auf den Gegner gibt. Dabei hilft insbesondere die Lernfähigkeit, um eine technologische Überlegenheit und damit eine Überlegenheit auf dem Schlachtfeld zu erlangen.

Anwendungsspezifische KI übernimmt bereits in Waffensystemen als Steuerungs- oder Assistenzeinheit Aufgaben wie Navigation, Zielerkennung und -identifikation sowie Angriffsplanung und -ausführung. Sei es die Drohne Taranis des britisches Herstellers BAE Systems, welche in einem neu hinzugefügten Flugmodus Routen entwirft und eigenständig nach Zielen sucht, bis das übergeordnete Missionsziel erreicht ist. Oder es sei der Geschützturm Super aEgis II des Herstellers DoDaam Systems genannt, welcher selbstständig Ziele identifiziert, anvisiert, verfolgt und die Entscheidung zum Feuern trifft. Aufgrund von Befürchtungen der Kunden, das Systeme könne Fehler machen, kann der Grad der Autonomie eingestellt werden. Als letzten Beispiel sei die KI „Alpha“ beschrieben, welche bisher nur in Simulationen aktiv gegen US Air Force Piloten angetreten ist und dabei zugleich Geschossen auswich, auf mehrere feindliche Ziele feuerte, sich an koordinierten Manövern mit befreundeten Piloten beteiligte sowie feindliche Taktiken registrierte, lernte und reagierte. Die KI *Alpha* und eine Ankündigung des Rüstungskonzerns Kalaschnikow, maschinelles Lernen in Waffensystem nutzen zu wollen, zeigen, dass die Fähigkeit in zukünftige Systeme integriert wird. Ob bereits in operierenden Waffensystemen maschinelles Lernen eingesetzt wird, ist Berichten über die Systeme nicht zu entnehmen. Es zeigt sich aber auch, dass sich die ersten Anwendungen im digitalen Raum, im Luftraum oder in statischen Verteidigungssystemen finden, da die Umgebung, in der die KI operieren muss, vergleichsweise weniger komplex als im Boden- oder Häuserkampf ist. Die Entwicklungspotentiale sollten jedoch nicht darüber hinwegtäuschen, dass KI das befähigende Element dieser Waffensysteme ist und damit der zu regulierende Faktor.

Kontrollerschwerende Eigenschaften und neue Ansatzpunkte

Wenn nun KI als das zu kontrollierende Element in Waffensystemen gilt, dann stellt sich die Frage, welche Eigenschaften von KI für eine qualitative oder quantitative Begrenzung genutzt werden können. Die traditionelle Rüstungskontrolle begrenzt die Anzahl an militärischen Fahrzeugen und Waffensystemen unter anderem aufgrund des äußerlich sichtbaren Erscheinungsbildes. Doch wie bei chemischen, biologischen oder radiologischen Stoffen existiert auch bei Software keine physische Manifestierung. Der Mensch braucht technische Hilfsmittel, um diese Stoffe bzw. die Software wahrzunehmen. Das äußere Erscheinungsbild kann demnach kein Ansatzpunkt sein.

Eine weitere Möglichkeit ist die Beschränkung anhand der inneren Funktionsweise. Antipersonenminen oder Streumunition werden beispielsweise aufgrund der mangelnden Unterscheidung zwischen Kombattanten und Zivilisten verboten. Doch die innere Funktionsweise von KI ist intransparent und nicht nachzuvollziehen. Zwar könnte der Quellcode analysiert werden, doch schon dieser Schritt wird erschwert, da der aus Systemen extrahierte Code in Maschinensprache vorliegen würde und eine Rekonstruktion zu Hochsprache schwierig bis unmöglich wäre. Doch selbst wenn der Quellcode vorliegen würde, gäbe es bei der Nutzung von maschinellem Lernen die Hürde eines nicht nachvollziehbaren Lernmodells. Die Lernmethode der *Deep Neural Networks* liefert keine Begründung für die berechneten Ergebnisse und die Komplexität des Modells macht es unmöglich, Entscheidungen im Voraus zu determinieren, wie es bei der simplen Funktionsweise von Antipersonenminen oder Streumunition der Fall ist. KI bzw. maschinelles Lernen ist inhärent intransparent und kann daher nicht aufgrund der inneren Funktionsweise beschränkt werden.

Rüstungskontrolle kann auch die äußerlich sichtbaren Fähigkeiten einer Waffe zur Beschränkung nutzen. Beispielsweise verbietet der Kernwaffenteststop-Vertrag, sobald er in Kraft tritt, die Durchführung von Kernwaffenexplosionen für zivile oder

militärische Zwecke. An dieser Stelle ist nicht die Funktionsweise oder der Sprengkörper an sich verboten, sondern die Explosionsfähigkeit. Die Fähigkeiten einer KI können allerdings flexibel hinzugefügt oder entfernt werden. Wie bei herkömmlicher Software können über Updates oder eine offene Softwarearchitektur Sicherheitslücken geschlossen oder Funktionen hinzugefügt werden. So ist dies beispielweise schon bei dem F-35 Kampflugzeug des US-amerikanischen Militärs möglich. An das importierte Flugzeug kann die israelische Armee eigene Waffen anbringen und das System über eine App-Integration entsprechend erweitern. Somit könnten bei Inspektionen kritische Funktionen kurzzeitig hinzugefügt oder entfernt werden. Damit entfällt für die Rüstungskontrolle nicht nur ein Ansatzpunkt, sondern es macht auf die Debatte um das Verbot von autonomen Waffen nichtig, wenn Autonomie eine flexibel erweiterbare Fähigkeit ist.

Als letzten Ansatzpunkt für Rüstungskontrolle sei hier die Kontrolle anhand der Äußerlichkeiten des Trägersystems genannt. Es werden beispielsweise nicht die nuklearen Sprengköpfe, sondern die Trägerraketen für kurze und mittlere Reichweite quantitativ begrenzt. Als Kernelement ist KI in diesem Fall dem Sprengkopf gleichzusetzen und damit sind Drohnen, Roboter und andere Systeme das Trägersystem. Durch einheitliche Standards könnte dieselbe KI in unterschiedlichen Waffensystemen die Navigation, Zielerkennung oder Feuerentscheidung übernehmen. Demnach kann der Kern moderner Waffensysteme, KI, zu keinem festen Waffensystem assoziiert werden. Eine Limitierung eines Waffensystems würde nur den Transfer auf ein anderes System bewirken.

Welche Ansatzpunkte bleiben nun übrig? Nachdem Rüstungskontrolle weder an dem äußerlich sichtbaren Erscheinungsbild, der inneren Funktionsweise, den äußerlich sichtbaren Fähigkeiten oder dem Trägersystem ansetzen kann, bleibt nur die Kontrolle in der Entwicklung oder im Einsatz. Für eine Kontrolle in der Entwicklung existiert das bisher nicht umgesetzte Konzept der präventiven Rüstungskontrolle. Sie soll militärisch nutzbare Technologie, Stoffe oder dergleichen bereits bei Entwicklung oder Erprobung verbieten und damit die Umsetzung in Waffensysteme zu verhindern. Denkbar wäre beispielsweise ein Register für militärische Forschung und Entwicklung, welches Risken frühzeitig erkennen lässt. Sollte KI im Einsatz kontrolliert werden, so müssten strategische und taktische Ziele oder Handlungsmöglichkeiten des Systems beschränkt werden. Das von Jürgen Altmann vorgeschlagene Konzept der *Glass Box* könnte hier eine mögliche Option sein. Die Glass Box soll in allen Systemen integriert sein und alle Handlungen und Entscheidungen in einem Protokoll aufzeichnen. Das Protokoll selbst bleibt in Kontrolle des Staates, in dessen Besitz das Waffensystem ist. Doch ein Hash des Protokolls wird zentral bei einer internationalen Organisation gespeichert. Ein Hash ist eine Prüfsumme, die die Integrität bzw. Unveränderbarkeit des Protokolls garantiert. Bei Verdacht auf illegale Kampfhandlungen könnte das Protokoll angefordert werden und durch den Hash wäre erkenntlich, ob das Protokoll manipuliert wurde. Es existieren zwar vereinzelt Lösungsvorschläge von Wissenschaftlern, doch das frühe Stadium der Konzepte zeigt, dass die Akteure in der Rüstungskontrolle die Problematik nicht erkannt haben und in Zukunft vor der Herausforderung stehen werden, alternative Konzept zu erproben und vor allem politischen durchzusetzen.

Kriseninstabilität

Es wird in drei Stufen unterschieden, in welcher Form ein Mensch in den Entscheidungsprozess einer Waffe eingebunden werden kann: (1) *human in the loop* (semiautonom): Ein Mensch kann am Entscheidungsprozess teilhaben und bspw. dem Waffensystem ein Ziel vorgeben und einen Angriff befehlen. (2) *human on the loop* (autonom unter menschlicher Aufsicht): Das Waffensystem wählt das Ziel und führt einen Angriff eigenständig aus, wird jedoch von einem Menschen überwacht, der jederzeit intervenieren könnte. (3) *human out of the loop* (vollautonom): Das Waffensystem wählt das Ziel und führt einen Angriff eigenständig aus, ohne dass ein Mensch es überwachen oder intervenieren könnte. Eine KI mit hoch entwickelten Wahrnehmungs-, Lern-, und Schlussfolgerungsfähigkeiten kann Stufe 3 erreichen. Doch die schnellen autonomen Entscheidungen gefährden ein Ziel der Rüstungskontrolle – die Stabilität in einem Krisenfall.

Der Mensch ist langsam. Er muss Sprache ausformulieren, Gestik interpretieren oder emotionale Eindrücke verarbeiten. Genau auf diesen menschlichen Faktor zielt die Rüstungskontrolle, um Stabilität im Krisenfall zu verbessern. Beispielsweise dürfen Raketen nicht dauerhaft abschussbereit sein oder Sprengköpfe müssen separat von Raketen gelagert werden. Denn in dieser Zeit bietet sich dem Menschen drei deeskalierende Handlungsmöglichkeiten: (1) Validierung der maschinellen Meldung oder Empfehlung (Es existieren einige Fälle im Kalten Krieg, in denen Menschen technischen Fehlalarm identifizierten und eine Eskalation verhinderten), (2) Kommunikation mit dem Gegner für Verhandlungen oder Klärungen und (3) Abwägung der moralisch und rechtlichen Implikationen. Die Rüstungskontrolle nutzt diesen Faktor nicht nur, sondern stärkt ihn mithilfe von vertrauensbildenden Maßnahmen (z. B. Informationsaustausch, gemeinsame Militärübungen, Austauschprogramme oder direkte Kommunikationskanäle). Doch mit selbstständig agierenden Waffensystemen beschleunigt sich das Geschehen. Der Fall *Flash Crash* aus dem Jahr 2010 an der New Yorker Börse zeigt dies eindrücklich. Durch

Nico Lück

Nico Lück ...

Marktmanipulation entstand dort eine Abwärtsspirale von Verkäufen, die von Computerprogrammen in einer Geschwindigkeit getätigte wurde, sodass Menschen nicht rechtzeitig eingreifen konnten. Eine ähnlich gegenseitig eskalierende Spirale kann auch im Zusammentreffen von KI-gesteuerten Waffensystemen geschehen. Vorstellbar ist ein Szenario in dem zwei Drohnen in Konflikt geraten und selbständig vernetzte Waffensysteme als Unterstützung anfordern. Diese Systeme würden in eskalierende Kampfhandlungen eintreten, noch bevor ein Mensch die Situation erfasst und reagiert hätte.

Dass der Faktor Mensch auf dem Schlachtfeld minimiert wird, ist aus Perspektive der Rüstungskontrolle eine alarmierende Entwicklung. Zwar bieten eigenständig entscheidende Waffensysteme einen strategischen Vorteil auf dem Schlachtfeld, jedoch sollte das Bewusstsein zurückkehren, dass die Langsamkeit des Menschen eine gute Sache sein kann.

Rüstungskontrolle im Zugzwang

Es lässt sich feststellen, dass das Konzept der Rüstungskontrolle in einer Krise steckt und parallel eine neue Technologie aufkommt, deren komplexe und anpassungsfähige Datenanalysen neue technische Potentiale für Waffensysteme eröffnet. Daher wird KI in Zukunft das Kernelement moderner Waffensysteme sein. Sie ermöglicht unter anderem höhere Grade an Autonomie von Waffensystemen und minimiert damit den deeskalierenden Charakter des Menschen. Doch auch wenn auf der multinationalen Ebene der Rüstungskontrolle erkannt wird, dass KI das kontrollwürdige Element von Waffensystemen ist, dann bleibt der Mangel an möglichen Ansatzpunkten zur Regulierung. Da diese Entwicklung bereits heute absehbar ist, müssen Akteure der Rüstungskontrolle aktiv neue Konzept erproben, die KI gesteuerten Waffensysteme bereits in der Entwicklung oder im Einsatz kontrollieren.

FIfF e. V. – Rainer Rehak: Laudatio für den Sonderpreis

Jörg Pohle: Datenschutz und Technikgestaltung

Dissertation an der Humboldt-Universität zu Berlin

Kommen wir jetzt zu der letzten Verleihung eines Weizenbaum-Studienpreises für heute. Wie Ihr vielleicht bemerkt habt: Von den vier vergebenen, die eingangs erwähnt worden sind, haben wir jetzt den dritten, den zweiten und dem ersten vergeben. Es wird jetzt noch einer vergeben, und zwar gab es dazu verschiedene Ansichten innerhalb der Jury, so dass wir uns entschieden haben, dass wir diese Arbeit auszeichnen, einfach ohne Zahl.

Es geht um eine Dissertation mit dem Thema *Datenschutz und Technikgestaltung. Die Geschichte und Theorie des Datenschutzes aus informatischer Sicht und Folgerungen für die Technikgestaltung* im Fach Informatik an der Humboldt-Universität zu Berlin, an den damaligen Diplom-Informatiker Jörg Pohle; mittlerweile Dr. Jörg Pohle.

Die Art der Arbeit spiegelte sich nach unserer Ansicht gut in unserer internen Diskussion wider, und zwar hat sich das herunterkondensieren lassen auf die Frage: Was ist Informatik? Wo verlaufen die Grenzen? Bezeichnet man Informatik auf der einen Seite eher als technischen Ansatz in der formalisierten Welt, oder auf der anderen Seite, wie zum Beispiel Wolfgang Coy für eine Theorie der Informatik auch proklamiert hat, dass Informatik sich auch weit über die formalen Bestandteile ihrer selbst bewegen muss, sonst kann es selber auch keine ernst zu nehmende Informatik sein. Genau diese Diskussion hatten wir auch, bei der Diskussion über die Arbeit von Jörg Pohle.

Gerade Datenschutz und Technikgestaltung berührt viele Disziplinen und hat viele Elemente, von Rechtswissenschaften über sozialwissenschaftliche Ansichten hinaus, natürlich zu den informatischen Aspekten, und diese Arbeit an sich ist mit ihren 314 Seiten das sichtbare Ergebnis von sehr viel harter Arbeit, eine immense Arbeit, die sich dadurch auszeichnet, dass sie Diskussionen über den Datenschutz nachzeichnet und Fragen behandelt, wie: Was schützt der Datenschutz überhaupt? Was soll er tun, was tut er? Und sie zeichnet auch nach, wie sich Diskussionen über die Zeit hinweg verändert haben, und möchte – so haben wir das gelesen – auch gleichzeitig sagen, dass viele der Diskussionen, die wir heutzutage haben, schon geführt worden sind und – wie man einer süffisanten Fußnote auch entnehmen kann – schon mit Ergebnissen, die heute allerdings wieder vergessen worden sind.

Man könnte auch sagen, die Arbeit, die wir darin auch sehen und so wertvoll bepreisen wollen, ist, nachzuzeichnen, wie sich Ideen verändert haben und vielleicht unter anderem Namen noch einmal aufkamen, und dann zu erkennen, das sind gleiche oder ähnliche Überlegungen, wie sie schon einmal getroffen worden sind, in neuem Gewand. Diese Ähnlichkeiten herzustellen, verlangt natürlich einen weiträumigen Überblick über die Materie, und den kann man sowohl der Arbeit als auch dem Literaturverzeichnis ansehen.

In der Diskussion haben wir uns auch entschieden, zu sagen, eventuell wird da nicht jede oder jeder Lesende den Überlegungen zustimmen, aber wer sich überhaupt sinnvoll in den Diskussionen um den Datenschutz, Datenschutztheorie, Datenschutzrecht und auch Datensicherheit bewegen oder positionieren will, muss nicht allen Punkte in der Arbeit zustimmen, aber muss sie auf jeden Fall gelesen haben.

Das heißt, an dieser Stelle schon einmal ein Aufruf, wer in diese Richtung denkt und arbeitet – wie immer bei den Weizenbaum-Studienpreisen – ist das eine klare Leseempfehlung.

Das lässt sich auch sehr schön daran ablesen, dass der erste Satz der Zusammenfassung lautet: „Ziel der vorliegenden Arbeit ist es, die historische Konstruktion des Datenschutzproblems, das Datenschutzes als seiner Lösung sowie die Architektur seiner rechtlichen Implementation aufzudecken und einer kritischen Revision aus informatischer Sicht zu unterziehen, um da-

raus Folgerungen für die Technikgestaltung zu ziehen", und der erste Satz der Einleitung – und das wird sehr gut die Diskussion, die sowohl in der Jury stattgefunden hat als auch die Diskussionen, die sich sicherlich noch anschließen können, gut darstellen – lautet: „Diese Arbeit verfolgt das Ziel, dem *Major Consensus Narrative* zum Datenschutz zu widersprechen."

Was genau das bedeutet, werden wir jetzt gleich angerissen sehen von Jörg Pohle – ich bitte Dich auf die Bühne, für die Überreichung zunächst, und dann für den Vortrag.

Jörg Pohle

Sonderpreis

Was wir aus der Geschichte der Datenschutzdebatte für die Technikgestaltung lernen können

Der vorliegende Beitrag soll in aller Kürze einen Überblick darüber geben, was der Hintergrund meiner Dissertation Datenschutz und Technikgestaltung *(Pohle 2018) ist, also warum ich mich damit beschäftigt habe, was meine Forschungs- und Erkenntnisinteressen sind, um dann zu klären: Was ist, was soll Datenschutz? Oder in der Sprache der Informatik: Was ist das Bedrohungsmodell, das dem Datenschutz zugrunde liegt? Diese Fragestellungen können auf eine lange historische Tradition zurückblicken und wurden sehr stark auch von Personen geprägt, die im FIfF oder im Umfeld des FIfF aktiv waren oder noch aktiv sind. Abschließend will ich kurz meinen Vorschlag für ein Vorgehensmodell mit einem analytischen Framework präsentieren, mit dem man solche sozio-technischen Systeme in der Entwicklung und für die Entwicklung analysiert und dann datenschutzgerecht – was sich nicht unbedingt in Datenschutzrechtskonformität erschöpft – entwerfen, entwickeln, umsetzen und einsetzen kann.*

Zentraler Hintergrund der Arbeit ist die Erkenntnis, dass privacy, surveillance und Datenschutz *essentially contested concepts* sind (zum Konzept siehe Gallie 1956, zur diesbezüglichen Einordnung von *privacy* siehe Mulligan, Koopman und Doty 2016). Weder in der wissenschaftlichen noch in der politischen Debatte gibt es eine Einigung zu unzähligen Aspekten, die grundlegend für das Verständnis der Problemlage und die Entwicklung von Lösungsansätzen sind. Schon auf der Ebene der Bestimmung des Phänomenbereichs gibt es massive Diskrepanzen zwischen den Beschreibungen, den Einordnungen und Erklärungen, die von verschiedener Seite geliefert werden. Während am einen Ende des Spektrums zwischenmenschliche Beziehungen zum Ausgangspunkt der Analyse gemacht werden, richtet sich der Blick am anderen Ende auf die strukturellen Bedingungen der modernen, funktional differenzierten Gesellschaft. Nicht überraschend ist es daher, dass es auch keine Einigung über das Schutzgut gibt: Von individuellen Bedürfnissen oder Interessen wie Privatheit, Vertraulichkeit, Eigentum, Entscheidungsfreiheit oder Persönlichkeitsentfaltung über soziale Konstruktionen wie Menschenwürde, Fairness oder Kommunikationsschutz bis zu gesellschaftlichen oder strukturellen Eigenschaften wie Freiheitsräumen, der Informationsordnung oder der Aufrechterhaltung der funktionalen Differenzierung der Gesellschaft wird alles vertreten. Gleiches gilt für die möglichen Gründe, Auslöser oder Verstärker der Gefährdung der betreffenden Schutzgüter: Ob technische Artefakte wie Daten, Informationen oder gar der Computer selbst, Praktiken wie Überwachung, Veröffentlichung, Verdatung, Missbrauch, Informationsverarbeitung oder -nutzung, Akteurskonstellationen oder deren Eigenschaften wie Machtasymmetrien, oder Phänomene auf der gesellschaftlichen Ebene wie die Digitalisierung aller Lebensbereiche, die globale Vernetzung oder die Industrialisierung der gesellschaftlichen Informationsverarbeitung – alles ist schon einmal als Gefahr oder Gefährder, Risiko oder Risikoquelle identifiziert worden.

Vor diesem Hintergrund überrascht es vielleicht ein wenig, dass die Auseinandersetzung um Datenschutz – gleiches gilt für privacy- oder Privatheitsschutz – in den letzten fünfzig Jahren eine extrem große Zahl von Gesetzen hervorgebracht hat. Die naheliegende Annahme, dass es dabei jeweils zu Einigungen gekommen ist, trügt jedoch, wie etwa der Vortrag von Kirsten Bock und Malte Engeler auf der FIfFKon 2018 mit Blick auf die EU-Datenschutzgrundverordnung gezeigt hat: Obwohl es Einigungen auf einen gemeinsamen Gesetzestext gibt, bleibt die Frage, was die Einzelregelungen jeweils bedeuten, wie sie also auszulegen sind, extrem umstritten.

Jörg Pohle bei der Präsentation seiner Arbeit

Hinzu kommt an vielen Stellen und immer häufiger, sowohl in der Öffentlichkeit wie in Gesetzen, die Forderung, privacy oder Datenschutz in Technik umzusetzen, ob als *Privacy by Design*, *Datenschutz by Design* oder *Privacy-Enhancing Technologies*. Was ich in meiner Arbeit festgestellt habe, ist, dass auch die Debatten um eine technische Umsetzung des Datenschutzes schon seit mindestens den 1960er Jahren laufen. So zeigt sich etwa, dass die heute verbreitet zu hörende Forderung, dass *privacy* oder Datenschutz schon in frühen Phasen der Technikentwicklung mit einzubeziehen sei, bereits im Jahr 1965 erhoben wurde (Baran 1965) – sehr weit, so scheint es, sind wir damit also noch nicht gekommen.

Forschungs- und Erkenntnisinteresse

Mein Forschungs- und Erkenntnisinteresse hat sehr viel damit zu tun, dass es sich um ein im Wesentlichen ungeordnetes Feld handelt: Ich habe untersucht, wie historisch eine Menge von Problemen konstruiert wurde, Probleme, die je nach Theorieschule oder -strömung wahlweise als *privacy*-, *surveillance*- oder Datenschutzprobleme bezeichnet werden, und wie dann jeweils Antworten, Verfahren und Techniken konstruiert wurden, die diese identifizierten Probleme beseitigen oder vermeiden sollen. Ich habe analysiert, welche Akteure in diesen Theorien und Debatten jeweils betrachtet wurden und werden – und welche nicht –, welche Beziehungen zwischen den Akteuren unterstellt wurden und werden, welche Interessen, Eigenschaften, Kenntnisse oder Fähigkeiten ihnen jeweils zugeschrieben – oder gerade ausgeblendet – wurden und werden, wie deren Informationsverarbeitung und Entscheidungsfindung adressiert wurde und wird, welche Rolle dabei jeweils informationstechnischen Systemen zugeschrieben wurde und wird, und welche Folgen sich daraus ergeben sollen – für Individuen, Gruppen, Organisationen, Institutionen oder die Gesellschaft insgesamt. Darauf aufbauend habe ich untersucht, wie auf der Basis der Problemidentifikation, die eine Konstruktion des Problems ist, dann jeweils identifiziert wird, wie gerade dafür dann passende Lösungen – und dabei vor allem auch Lösungen in Technik – aussehen sollen. Auf der Basis dieser Analysen konnte ich dann ermitteln, was davon aus informatischer Sicht überhaupt oder überhaupt noch haltbar ist, und was daraus für die Gestaltung informationstechnischer Systeme gelernt werden kann.

Seit mehr als fünfzig Jahren beschäftigt sich die Informatik mit diesem Thema. Die ersten dezidiert informatischen Beiträge dazu sind Mitte der 1960er Jahre erschienen (siehe etwa die Beiträge in Rector 1965). Dennoch diskutieren wir immer noch und immer wieder über die gleichen Grundlagen und Grundfragen. Das liegt nicht zuletzt daran, dass es eine relativ schwache theoretische Basis gibt. In der Informatik wird dann sehr gerne einfach irgendetwas – irgendeine Theorie oder auch nur ein Theoriefragment – herausgegriffen, das zum Objekt der technischen Umsetzung gemacht wird. Am Ende sind die Beteiligten ganz stolz darauf, dass sie die Umsetzung beweisen können. Das ist absurd: Angesichts der Vielzahl untereinander umstrittenen Vorstellungen davon, worum es gehen soll, eine Theorie oder einen Ansatz herauszugreifen – beliebig und ohne jede Begründung – und dann stolz zu verkünden, diese seien beweisbar umgesetzt. Informatisch lässt sich das so reformulieren: Wir nummerieren die Theorien und Vorstellungen einfach durch, von 1 bis n. Dann wählt jemand *privacy7* und baut dafür Technik, das heißt eine „*Privacy7*-Enhancing Technology". Aber niemand hinterfragt die Behauptung, dieses System stelle zugleich eine Lösung für *privacy3* oder für *privacy11* dar …

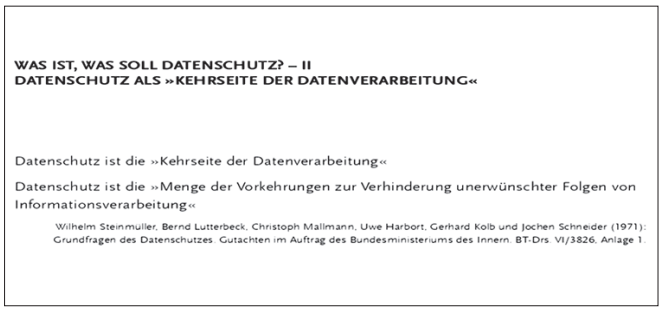
Der Schwerpunkt meiner Arbeit lag dabei auf dem Verständnis von Datenschutz, wie es historisch vor allem in Deutschland und vor allem in den 1970er Jahren im Umfeld der damaligen Rechtsinformatik, oder besser: Rechtskybernetik, konzeptualisiert wurde. Das hatte nicht zuletzt auch einen großen Einfluss auf die ursprüngliche Architektur des Datenschutzrechts. Personen, an die in diesem Zusammenhang zu erinnern lohnt, sind etwa Wilhelm Steinmüller, Adalbert Podlech – beide waren etwa auch Kläger gegen das Volkszählungsgesetz –, Herbert Fiedler oder Klaus Lenk.

Was ist, was soll Datenschutz?

Die wichtigste Erkenntnis der Vorarbeiten aus den 1970er Jahren lautet, dass der Ausgangspunkt einer informatisch fundierten Analyse der individuellen und gesellschaftlichen Auswirkungen moderner, automationsgestützter, zunehmend automatisierter und tendenziell industrialisierter Informationsverarbeitung die realen Informationsverarbeitungsprozesse, -praxen und -techniken in Organisationen und der Gesellschaft sein muss. Und zumindest damals wurde Datenschutz nicht einfach nur als Schutz von Privatheit verstanden, sondern als „Kehrseite von Datenverarbeitung", nämlich als „Menge der Vorkehrungen zur Verhinderung unerwünschter Folgen von Informationsverarbeitung" (Steinmüller u. a. 1971). Dabei handelt es sich um ein dezidiert politisches Programm, formuliert von der Gruppe um Wilhelm Steinmüller 1971 im *Gutachten Grundfragen des Datenschutzes* für das Bundesministerium des Innern. Diese Zielvorstellung geht weit über das hinaus, was heute unter Labels wie *privacy*, *Privatheit* oder *surveillance* diskutiert wird. Es geht um den Schutz von Einzelnen wie von gesellschaftlichen Gruppierungen, es geht aber auch um den Schutz staatlicher oder gesellschaftlicher Institutionen, etwa des Parlaments oder der kommunalen Selbstverwaltung, der Demokratie, des Rechtsstaats oder des Sozialstaats, denn als unerwünscht kann jede Folge von Informationsverarbeitung gelten, die den Zielen der Gesellschaft zuwiderläuft, Zielen, die wir uns als Gesellschaft gesetzt haben, etwa im Grundgesetz, der Europäischen Menschenrechtskonvention oder in der EU-Grundrechtecharta. Es geht, wie Wilhelm Steinmüller es am Ende seines Lebens formulierte, nicht um Privatsphäre, sondern um die gesellschaftliche Kontrolle von Technik (siehe das Video-Interview Rost und Krasemann 2009). Es geht ebenso um Öffentlichkeit; es geht um den Schutz der Öffentlichkeit vor „Verdatung" (Dammann 1974). Es geht, wie die Arbeit zeigt, um die politische Deliberation, es geht um das Funktionieren aller anderen autonomen gesellschaftlichen Bereiche oder Subsysteme, die jeweils eigene Funktionslogiken haben, vor der Unterwerfung unter die Funktionslogiken derjenigen, die die Technik, die Technikgestaltung und den Technikeinsatz kontrollieren (dazu zusammenfassend Pohle 2018, S. 249 ff.). Es geht auch nicht nur um personenbezogene Daten, denn es ist keineswegs besser oder wünschenswerter, wenn Grundrechte oder Grundfreiheiten oder Rechtsstaat und Demokratie mit anonymen oder statistischen Daten verletzt werden (ausführlich zum problematischen Umgang mit Personenbezug und Anonymität von Informationen S. 171 ff.). Es geht auch nicht nur um Daten, sondern auch um Prozesse, also organisationseigene Entscheidungsprogramme, oder Interaktions- und Entscheidungsarchitekturen wie User Interfaces, kurz: alles, was der Welt „entnommen" und in Modelle verwandelt wird, die dann in die Technik „gesteckt", also eingeschrieben, werden (früh schon Fiedler 1975, siehe dazu auch den Beitrag von Guagnin & Pohle in Ausgabe 1/2019 der *FIfF-Kommunikation*).

Was ist also das (abstrakte) Bedrohungsmodell, das dem Datenschutz zugrunde liegt? Erstens geht es darum, Informationsmacht unter Kontrolle zu bringen. Informationsmacht erwächst etwa aus der Verstärkung der Fähigkeit zur Kontrolle oder Beeinflussung individueller, kollektiver und institutioneller Betroffener und ihrer Kommunikationen, Entscheidungen und Handlungen (Pohle 2018, S. 247 ff.). Es geht zweitens darum zu verhindern, dass es zu Rationalitätsverschiebungen zugunsten derjenigen kommt,

die die Technik gestalten oder einsetzen (S. 249 f.). Organisationen bedrohen die – die moderne, funktional differenzierte Gesellschaft prägende – Trennung zwischen gesellschaftlichen Subsystemen oder Feldern mit Kontexten und ihren jeweils spezifischen Eigenschaften und Eigenlogiken, weil sie diese ihrer eigenen Organisationslogik unterwerfen (S. 250 f. sowie ausführlich Rost 2008). So produziert etwa Facebook nicht einfach Öffentlichkeit, sondern eine Öffentlichkeit nach Facebooks Vorannahmen und Vorgaben. Und drittens gilt es zu verhindern, dass es zu Kontingenzverlust für Betroffene kommt: indem Organisationen Entscheidungsarchitekturen gestalten und Handlungsmöglichkeiten prästrukturieren (Lenk 1982), indem sie auf der Basis der Vergangenheit, wie sie sich in den zugrunde gelegten Information, d. h. Modellen, widerspiegelt, in der Gegenwart über Zukunft disponieren (Luhmann 1990). Sie fesseln damit an die Vergangenheit, wie sie von den Organisationen selbst erzeugt wurde, und blockieren Möglichkeiten für Betroffene, sich in der Zukunft anders zu entscheiden (so schon früh Podlech 1972).



Datenschutz heißt also, informationell begründete soziale Macht in der Informationsgesellschaft unter Bedingungen zu stellen, sie zu zwingen, sich zu verantworten, und sie damit – wieder oder überhaupt erst einmal – gesellschaftlich verhandelbar zu machen. Die Funktion des Datenschutzes besteht darin, dass kontingente Sozialstrukturen sich auch unter den Bedingungen der zunehmenden „Industrialisierung der gesellschaftlichen Informationsverarbeitung" (Steinmüller 1981) und gegen die überlegene „Strukturierungsmacht" (Rost 2014) von Organisationen reproduzieren können.

Vorgehensmodell und analytisches Framework

Eine allgemeine „Lösung" des Datenschutzproblems kann es ebenso wenig geben wie ein allgemeines, gleichwohl stets passgenaues, Bedrohungsmodell. Das abstrakte Bedrohungsmodell muss immer auf den konkreten Kontext, in dem das zu gestaltende System eingesetzt werden soll, zugeschnitten werden, denn konkrete Bedrohungen lassen sich nur anhand konkreter Informationssysteme identifizieren. Daher bedarf es eines prozeduralen Operationalisierungsansatzes, der diese Zuschneidung leistet, der es erlaubt, darauf basierend konkrete, materielle Anfordungen abzuleiten und für die Systemgestaltung nutzbar zu machen (ausführlich zu Angreifer-, Bedrohungs- und Vorgehensmodell Pohle 2018, S. 257 ff.). Überprüfbarkeit ist dabei nur dann gegeben, wenn die Zwischenprodukte – das sind nachfolgend die Anwendungsbereichsbestimmung, die Akteursanalyse sowie die Interessen-, Zweck- und Machtanalyse – transparent gemacht werden müssen.

Im ersten Schritt ist der Anwendungsbereich des zu gestaltenden oder des zu prüfenden Verfahrens oder – im Rahmen von Technikgestaltung oder Technikprüfung – des informationstechnischen Systems festzulegen oder zu bestimmen.

Im zweiten Schritt sind die beteiligten oder zu beteiligenden AkteurInnen zu identifizieren und zu beschreiben. Dazu zählen nicht nur die Organisation und deren MitarbeiterInnen, „Verdatete" (Steinmüller 1988) und eventuelle Dritte, sondern gerade auch relevante Teilgruppen, also etwa Admins oder einfache UserInnen als klassische Typen von MitarbeiterInnen, Gruppen von Betroffenen nach den unterschiedlichen Risiken, denen sie ausgesetzt sind, oder AngreiferInnen nach ihren ökonomischen, politischen oder anderen Interessen. Für diese AkteurInnen ist dabei zu identifizieren, in welchen Rollen sie auftreten. Damit sind nicht nur die gesellschaftlich konstruierten Rollen wie Individuum, Subjekt, Familienmitglied, BürgerIn, KundIn, PatientIn oder MandantIn für Menschen – als Personenkonzepte – oder Behörde, Unternehmen oder Presse für Organisationen gemeint, sondern auch die konkreten Handlungsrollen wie TechnikgestalterIn, Admin, AnbieterIn, NutzerIn, in denen sie jeweils miteinander und mit der Technik interagieren. Anhand dieser Rollen lassen sich dann sowohl gesellschaftlich geprägte Erwartungen und gesellschaftlich konsentierte Interessen identifizieren und zuweisen, also die Freiheits- und Partizipationsversprechen der modernen bürgerlichen Gesellschaft und sogar ihre Strukturschutzprinzipien und -mechanismen, wie auch individuelle oder kollektive Erwartungen und Interessen der jeweiligen AkteurInnen. Anschließend sind die Zwecke zu identifizieren, die die AkteurInnen jeweils verfolgen, gleich ob es interpersonale, politische, ökonomische oder andere Zwecke sind.

Im dritten Schritt sind daher die Interessen und Zwecke vor dem Hintergrund, in welchem Verhältnis die AkteurInnen zueinander stehen, vor allem in welchem Machtverhältnis, und inwieweit sie voneinander abhängig sind, etwa von der Erbringung einer spezifischen Leistung wie der Bereitstellung einer Kommunikationsinfrastruktur für die Kommunikation mit anderen, zueinander in Beziehung zu setzen und zu analysieren. In dieser Interessen-, Zweck- und Machtanalyse muss deutlich werden, inwieweit die Interessen und Zwecke der unterschiedlichen AkteurInnen einander entsprechen, kompatibel sind oder einander widersprechen, welche Interessen und Zwecke nur durchgesetzt oder erreicht werden können, wenn andere AkteurInnen kooperieren, von welchen AkteurInnen Kooperation zu erwarten ist und von welchen nicht. Darüber hinaus ist zu analysieren, welche Folgen sich für die Machtbeziehungen zwischen den AkteurInnen ergeben oder ergeben können, wenn AkteurInnen ihre Interessen und Zwecke auch gegen die Interessen und Zwecke anderer AkteurInnen durchzusetzen in der Lage sind. Anschließend sind diese Interessen und Zwecke zu gewichten und zu bewerten, um darauf basierend zwischen den widerstreitenden Interessen und Zwecken abzuwägen. Datenschutz steht dabei konsequent aufseiten der strukturell schwächeren AkteurInnen und schreibt sich die Durchsetzung ihrer Interessen gegen die Interessen der ungleich mächtigeren Organisationen auf die Fahne, und in diesem Sinne sind auch Gewichtung, Bewertung und Abwägung vorzunehmen.

Im Systementwicklungsprozess darf erst an dieser Stelle die eigentliche Zwecksetzung für das zu entwickelnde System vorge-

nommen werden, damit sie selbst zum diskutierbaren Teil der das System definierenden Vorentscheidungen wird. Damit wird zugleich das Problem der Zweckspezifizierung, also die Frage, wie abstrakt oder konkret, wie weit oder eng der Zweck festzulegen ist, lösbar. Die Entscheidungsheuristik lautet dann: Je divergenter die Interessen und Zwecke sind, desto konkreter muss der Zweck spezifiziert werden. Je asymmetrischer das Machtverhältnis ist, desto enger muss der Zweck definiert werden.

Die anwendungsbereichsspezifische Bedrohungsanalyse stellt den vierten Schritt dar und dient der Erzeugung des konkreten, anwendungsbezogenen Bedrohungsmodells, indem sie das abstrakte Bedrohungsmodell (das umfassend dargestellt wird in Pohle 2018, S. 260 ff.) vor dem Hintergrund der vorherigen Analysen spezifiziert, und der Ableitung von materiellen wie prozeduralen Anforderungen.

Erst auf dieser Basis lässt sich dann für die identifizierten Bedrohungen entscheiden, wie informationstechnische Lösungen zu gestalten sind, welche existierenden informatischen Artefakte – Frameworks, Module, Codefragmente – dabei für die konkreten Bedrohungen geeignete Lösungen sind und darum ausgewählt werden sollten – und welche nicht –, und welche Anforderungen sich für den Einsatz dieser Systeme ergeben, also etwa auch, welche nicht informatisch lösbaren Anteile der Probleme durch das soziale Umsystem, in das die Informationstechnik jeweils eingebettet ist, gelöst werden müssen.

Literaturverzeichnis

Baran, Paul (1965), „Communications, computers and people". In: Proceedings of the November 30–December 1, 1965, fall joint computer conference, part II: computers: their impact on society. AFIPS '65. New York, NY: ACM. 45–49.

Dammann, Ulrich (1974), „Strukturwandel der Information und Datenschutz". In: Datenverarbeitung im Recht 3 (3/4): 267–301.

Fiedler, Herbert (1975), „Datenschutz und Gesellschaft". In: GI – 4. Jahrestagung, herausgegeben von D. Siefkes. Berlin: GI / Springer. 68–84.

Gallie, Walter Bryce (1956), „Essentially Contested Concepts". In: Proceedings of the Aristotelian Society, New Series, 56: 167–198.

Lenk, Klaus (1982), „Information Technology and Society". In: Microelectronics and Society. For Better or for Worse. A Report to the Club of Rome, herausgegeben von Günter Friedrichs und Adam Schaff. Oxford: The Club of Rome, Pergamon Press. 273–310.

Luhmann, Niklas (1990), „Risiko und Gefahr". In: Soziologische Aufklärung: Konstruktivistische Perspektiven, Band 5. Opladen: Westdeutscher Verlag. 131–168.

Mulligan, Deirdre K., Koopman, Colin und Doty, Nick (2016), „Privacy is an essentially contested concept: a multi-dimensional analytic for mapping privacy". In: Philosophical Transactions of the Royal Society of London A: Mathematical, Physical and Engineering Sciences 374 (2083). DOI: 10.1098/rsta.2016.0118.

Podlech, Adalbert (1972), „Verfassungsrechtliche Probleme öffentlicher Informationssysteme". In: Datenverarbeitung im Recht 1: 149–169.

Pohle, Jörg (2018), „Datenschutz und Technikgestaltung: Geschichte und Theorie des Datenschutzes aus informatischer Sicht und Folgerungen für die Technikgestaltung". Dissertation, Mathematisch-Naturwissenschaftliche Fakultät, Humboldt-Universität zu Berlin. DOI: 10.18452/19136. URL: https://edoc.hu-berlin.de/handle/18452/19886.

Rector, Robert W. (Hrsg.) (1965), Proceedings of the November 30–December 1, 1965, fall joint computer conference, part II: computers: their impact on society. AFIPS '65. New York, NY: ACM.

Rost, Martin (2008), „Gegen große Feuer helfen große Gegenfeuer – Datenschutz als Wächter funktionaler Differenzierung". In: vorgänge, Nr. 4: 15–26.

Rost, Martin (2014), „Neun Thesen zum Datenschutz". In: Fundationes I: Geschichte und Theorie des Datenschutzes, herausgegeben von Jörg Pohle und Andrea Knaut. Münster: Monsenstein und Vannerdat. 37–44.

Rost, Martin und Krasemann, Henry (2009), Interview mit Wilhelm Steinmüller. Interviews zur Geschichte und Programmatik des Datenschutzes in Deutschland. URL: https://www.datenschutzzentrum.de/interviews/steinmueller/.

Steinmüller, Wilhelm (1981), „Die Zweite industrielle Revolution hat eben begonnen – Über die Technisierung der geistigen Arbeit". In: Kursbuch 66: 152–188.

Steinmüller, Wilhelm (Hrsg.) (1988), Verdatet und vernetzt. Sozialökologische Handlungsspielräume der Informationsgesellschaft. Frankfurt am Main: Fischer Taschenbuch Verlag.

Steinmüller, Wilhelm et al. (1971), Grundfragen des Datenschutzes. Gutachten im Auftrag des Bundesministeriums des Innern, BT-Drs. VI/3826, Anlage 1.

Jörg Pohle

Dr. **Jörg Pohle** ist PostDoc am Alexander von Humboldt Institut für Internet und Gesellschaft in Berlin, wo er das Forschungsprogramm *Daten, Akteure, Infrastrukturen* coleitet und sich unter anderem mit gesellschaftlichen Aushandlungen im Bereich Privacy, Surveillance, IT-Sicherheit und Datenschutz befasst. Sein Forschungsinteresse gilt dem Schnittbereich von Informatik und Recht, dem Feld Informatik und Gesellschaft, der Modellifizierung und ihren gesellschaftlichen Auswirkungen sowie dem Datenschutz durch Technikgestaltung.

Jörg Pohle studierte Rechtswissenschaft, Politikwissenschaft und Informatik in Berlin. Seine Diplomarbeit beschäftigte sich mit der Sicherheit von und dem Sicherheitsdiskurs zu Wahlcomputern. Er promovierte bei Wolfgang Coy an der Humboldt-Universität zu Berlin über Geschichte und Theorie des Datenschutzes aus informatischer Sicht und Folgerungen für die Technikgestaltung.

NETZPOLITIK.ORG

Alexander Fanta, Ingo Dachwitz, Tomas Rudl, Chris Köver, Arne Semsrott, Matthias Monroy, Markus Beckedahl

Zwischen DSGVO und Uploadfiltern: Das war Europas Netzpolitik der letzten fünf Jahre

Mehr Datenschutz, Milliardenstrafen gegen Konzerne und Uploadfilter gegen alles: Unter Kommissionspräsident Jean-Claude Juncker und einem selbstbewussten EU-Parlament war Europas Digitalpolitik ein Wechselbad der Gefühle. Wir schauen auf die wichtigsten Gesetze und Geschehnisse zurück.

Die Europäische Union hat in den vergangenen Jahren entscheidende Weichenstellungen für die Netzpolitik der Zukunft getroffen – leider nicht immer in die richtige Richtung. Seit der Europawahl 2014, dem Amtsantritt von EU-Kommissionschef Jean-Claude Juncker und der 2015 vorgestellten Strategie für einen digitalen Binnenmarkt[1] blieb praktisch kein Stein mehr auf dem anderen. Die EU verbesserte den Datenschutz und teilte Milliardenstrafen an einige Digitalkonzerne aus, sieht aber zugleich Uploadfilter als Wundermittel gegen alles und vernetzt die behördliche Datensammelei auf bedenkliche Art und Weise. Wir fassen die wichtigsten Meilensteine der vergangenen Jahre zusammen.

- Uploadfilter, Terrorfilter und neue Gefahren
- Datenschutz: Erst große Schritte, dann Stillstand
- Strafen gegen Tech-Konzerne, aber keine Digitalsteuer
- Infrastruktur: Roaming-Gebühren abgeschafft, Netzneutralität überwiegend erhalten
- Gemeinsam auf dem Weg zu mehr Überwachung
- Maschinelles Lernen: Ethische Richtlinien, aber keine Regulierung
- Etwas mehr Schutz für Hinweisgeber
- Lobbying und Desinformation
- Fazit: Geht wählen, es war nie wichtiger!

Uploadfilter, Terrorfilter und neue Gefahren

Die Urheberrechtsreform der EU schränkt die Bewegungsfreiheit im Netz deutlich ein. Sie zwingt alle EU-Mitgliedstaaten in den nächsten zwei Jahren dazu, Online-Plattformen gesetzlich zum Filtern von Nutzer-Inhalten zu verpflichten. Sie schreibt zudem ein EU-weites Leistungsschutzrecht vor, das selbst kurze Anreißertexte auf Links zu Medienseiten vergütungspflichtig macht.

Die Europäische Union beschloss[2] die Reform im März – trotz erbittertem Widerstand von NetzaktivistInnen (Hier unsere Chronologie[3]). Der EU sei es dabei nicht gelungen, dem Urheberrecht ein zeitgemäßes Update zu verpassen und die Interessen einer breiten Schicht von neuen Urhebern zu berücksichtigen, kommentierte netzpolitik.org-Chefredakteur Markus Beckedahl[4].

Das Urheberrecht setzt zudem ein negatives Vorbild: Ein Vorschlag der EU-Kommission könnte Uploadfilter auch gegen echte oder angebliche „terroristische Inhalte“[5] vorschreiben. Er soll nach der EU-Wahl beschlossen werden. NGO-Vertreter

Freiheit statt Angst Demo in Berlin, Foto: mw238 – CC BY-SA 2.0

fürchten zudem, in der nächsten Legislaturperiode könnte eine mögliche Änderung der e-Commerce-Regeln die zwar nicht ganz unproblematischen, aber bewährten Schutzmechanismen für die Meinungsfreiheit im Netz[6] aushebeln.

Datenschutz: Erst große Schritte, dann Stillstand

Starke Betroffenenrechte, einheitliche Regeln für alle in der Europäischen Union agierenden Unternehmen und echte Sanktionsbefugnisse für unabhängige Aufsichtsbehörden – das sind die wohl größten Stärken der 2016 verabschiedeten Datenschutzgrundverordnung. Mit dem Mammut-Gesetz hat die EU nicht nur gezeigt, dass sie in Sachen Digitalisierung sehr wohl Gestaltungsmacht hat, sondern auch den größten zusammenhängen Datenmarkt der Welt geschaffen. Nach einer Übergangsfrist wird die DSGVO seit 2018 angewendet. Legendär war sie schon vorher: Die noch in der vorigen Legislaturperiode begonnen Verhandlungen fanden unter so extremem Druck der Industrie[7] statt, dass sie den denkwürdigen Beinamen als „größte Lobby-Schlacht der EU“ bekam.

Am Ende stand eine Verordnung, der man ihren Kompromisscharakter zwar anmerkt, die aber deutlich den Stempel des EU-Parlaments trägt. Gemeinsam mit der Kommission konnten sich die Abgeordneten in einigen entscheidenden Punkten gegen bremsende Mitgliedstaaten[8] durchsetzen. So wurden unter anderem neue Instrumente wie die Datenschutz-Folgenabschätzung und

Privacy-by-Design geschaffen und die etablierten Grundsätze der Zweckbindung und der Datensparsamkeit fortgeschrieben – auch wenn Industrielobbyisten und das deutsche Innenministerium[9] dies gern verhindert hätten. Zu der Geschichte gehört allerdings auch: So epochal die Datenschutzgrundverordnung ist, so groß waren das Kommunikationsdebakel[10] und die Verunsicherung[11] in Deutschland rund um den Stichtag 25. Mai 2018.

Auch BürgerrechtlerInnen und Nichtregierungsorganisationen betonen, dass die DSGVO lediglich ein erster Schritt sei – wenn auch in die richtige Richtung. Nach dem Mammut-Projekt ging der EU in Sachen Datenschutz allerdings die Puste aus. Das Privacy Shield[12] – Nachfolger des 2015 vom EuGH gekippten Safe-Harbor-Abkommens[13] – soll europäische Kundinnen und Kunden von US-Firmen vor dem Zugriff der dortigen Geheimdienste auf ihre Daten schützen. Die Behauptung eines vergleichbar hohen Datenschutzniveaus bleibt aber auch Jahre nach den Snowden-Enthüllungen lachhaft. In der DSGVO festgelegte Möglichkeiten wie Standardisierung, Zertifikate oder Privacy-Icons zum einfacheren Verständnis von Datenschutzerklärungen trieb die EU-Kommission bisher kaum voran. Und über die Auslegung erläuterungsbedürftiger Rechtsbegriffe der Verordnung werden die Gerichte jahrelang verhandeln.

Klarheit für den Bereich Online-Tracking und strengere Regeln für die Anbieter digitaler Kommunikationsdienste hätte noch 2018 eigentlich die ePrivacy-Verordnung[14] bringen sollen. Trotz großer Datenskandale wie dem um Facebook und Cambridge Analytica[15] ist der Regulierungsmut der EU in den vergangenen zwei Jahren erheblich gesunken. Zumindest bei einigen EU-Akteuren. Denn während EU-Kommission und -Parlament sich bei der ePrivacy-Reform an den verabredeten Zeitplan hielten, waren es wiederum die Mitgliedstaaten im Rat[16], die das Verfahren aus Sorge vor Überregulierung und Schäden für die Wirtschaft[17] ausbremsten. Wie und ob die Verordnung nach den Wahlen verabschiedet wird, ist ungewiss[18].

Strafen gegen Tech-Konzerne, aber keine Digitalsteuer

EU-Wettbewerbskommissarin Margrethe Vestager trug sich mit Milliardenstrafen den Ärger der großen Tech-Konzerne ein. Allein Google bekam drei Strafen wegen illegaler Praktiken: im Jahr 2017 2,4 Milliarden Euro für den Missbrauch seine marktbeherrschenden Stellung durch Google Shopping[19], im Vorjahr 4,3 Milliarden Euro wegen Googles Praktiken bei Android[20] und zuletzt 1,5 Milliarden wegen Online-Werbung[21]. Apple erhielt 2016 eine Rekordstrafe von 13 Milliarden Euro[22] wegen illegaler Steuertricks in Irland. US-Präsident Donald Trump nannte Vestager deshalb gar die „Steuerlady" der EU[23] und warf ihr vor, die USA zu hassen.

Tatsächlich setzte Vestager mit den Strafen erste Schritte, die Dominanz der großen Digitalkonzerne einzudämmen. Andere Ideen zur Regulierung der Konzerne[24] warten hingegen auf Verwirklichung. Eine Bauchlandung machte die Digitalsteuer[25], die einen größeren Teil der Einnahmen der US-Konzerne an die EU-Staaten hätte abführen sollen. Die EU-Staaten begruben den Vorschlag[26] wenige Wochen vor der Wahl und wollen nun eine – wenig realistische – globale Lösung.

Infrastruktur: Roaming-Gebühren abgeschafft, Netzneutralität überwiegend erhalten

Nicht unberührt blieb das Fundament jeglicher Digitalisierung, die zugrundeliegende Infrastruktur. Hier hat sich die Kommission einiges vorgenommen und umgesetzt – wenn auch nicht ganz so wirtschaftsfreundlich, wie es sich der Ex-Digitalkommissar Günther Oettinger vorgestellt hatte.

Oettinger legte mehrere Initiativen selbst vor oder brachte offene Gesetzesvorschläge[27] der Vorgänger-Kommission von José Barroso unter Dach und Fach. Die Stoßrichtung war dabei immer klar: Europa brauche „digitale Champions", die groß genug sind, um sich auf dem Weltmarkt behaupten[28] zu können.

Im schlimmsten Fall wäre auf der einen Seite ein großteils deregulierter Telekom-Markt die Folge gewesen, den sich nur wenige verbliebene Konzerne unter sich aufteilen – und auf der anderen eine löchrige Netzneutralität mit Überholspuren für reiche Anbieter und Kunden, gedrosselten P2P-Protokollen und dem Kabel-TV ähnelnden Sub-Internet-Paketen.

Ganz so schlimm ist es zum Glück nicht gekommen, was zu einem guten Teil der Zivilgesellschaft zu verdanken ist. Deren rege Beteiligung[29] am Prozess hat wohl maßgeblich dazu beigetragen, dass die finalen Regeln zur Netzneutralität letztlich stark ausgefallen[30] sind. Zwar klafft mit nicht ausdrücklich verbotenen Zero-Rating-Angeboten ein ärgerliches Schlupfloch[31] in den Regeln, und manche EU-Länder, allen voran Deutschland, schlampen bei der Umsetzung einzelner Bestimmungen[32].

Unterm Strich kann die EU-Verordnung jedoch als Erfolg für ein freies und offenes Internet gelten, selbst wenn dieses an anderen Stellen zunehmend unter Druck gerät. Und diesen Erfolg kostete die EU-Kommission genüsslich aus, als die Trump-Administration im Vorjahr die „Open Internet Order" rückgängig machte[33], die in den USA bis dahin die Netzneutralität schützte. „Wir werden die Netzneutralität in Europa weiter verteidigen", versicherte etwa der Kommissions-Vizepräsident Andrus Ansip auf Twitter[34] oder in öffentlichen Auftritten[35]. Bleibt zu hoffen, dass die nächste Kommission sich das zum Vorbild nimmt und sieht, dass bürgerInnenfreundliche Politik, die allen zu Gute kommt, politisch einfacher zu verkaufen ist als eine, die nur die Industrie bedient.

Selbige EU-Verordnung schaffte überdies die horrenden Roaming-Gebühren innerhalb der EU ab[36] – ebenfalls ein populäres

Unterfangen. Telefonate aus dem Inland in ein anderes EU-Land machte allerdings erst eine andere Reform billiger: der Ende des letzten Jahres beschlossene Europäische Kodex für die elektronische Kommunikation.

Gemeinsam auf dem Weg zu mehr Überwachung

Die Möglichkeiten zur Überwachung der EU-BürgerInnen wachsen. Unter dem Stichwort „Interoperabilität" vernetzt die Europäische Union[37] ihre großen Datenbanken im Bereich Justiz und Inneres. Der endgültige Beschluss dazu fiel kurz vor der Europawahl. Die im Schengener Informationssystem (SIS II), Visa-Informationssystem und Eurodac gespeicherten Fingerabdrücke und Gesichtsbilder werden in einem „gemeinsamen Identitätsspeicher" abgelegt[38]. Dort werden sie mit einem „Europäischen Suchportal" prozessiert. Im Hintergrund läuft außerdem ein „Detektor für Mehrfachidentitäten", der nach Verknüpfungen zwischen den biometrischen Daten und ihnen zugeordneten Ausweisdokumenten sucht. Mit dem Projekt dürfte der polizeiliche Datenverkehr drastisch steigen, allein Europol rechnet mit 100.000 täglichen Abfragen seiner Dateien.

Nach der Europawahl plant die EU außerdem, den Zugriff auf elektronische Beweismittel drastisch zu erleichtern. Dafür soll es drei Schritte geben. Die „E-Evidence"-Verordnung"39 soll die polizeiliche Abfrage von Daten bei Internetfirmen[40] in anderen EU-Staaten deutlich erleichtern. Die EU-Staaten wollen Anbietern mit hohen Geldstrafen drohen[41], wenn diese nicht binnen weniger Stunden den Aufforderungen von Behörden nachkommen. Für Firmen mit Sitz in den USA plant die Kommission ein Durchführungsabkommen im Rahmen des „CLOUD Act"42, den die US-Regierung erlassen hat. Zusätzlich verhandelt auch der Europarat über die schnelle Herausgabe elektronischer Beweismittel. Die „Budapest-Konvention"[43] zur Kooperation bei Computerstraftaten soll um eine „Sicherungsanordnung" erweitert werden.

Für Aufregung sorgten indes zahlreiche andere Maßnahmen aus Brüssel. Beschlossen wurde etwa eine Pflicht zur Speicherung von Fingerabdrücken[44] und biometrischen Fotos in allen Personalausweisen. Behörden in ganz Europa könnten damit ihre biometrischen Datenspeicher ausbauen. Auch innereuropäische internationale Flugreisen werden dank einer 2016 beschlossenen Richtlinie[45] inzwischen engmaschig überwacht. Die EU macht zudem ab 2024 den Einbau von Blackboxen[46] zur Unfalldatenspeicherung in alle Neuwagen verpflichtend. Auch bei der Überwachung von Flugreisen

Maschinelles Lernen: Ethische Richtlinien, aber keine Regulierung

Zumindest Untätigkeit kann man der EU nicht vorwerfen, wenn es um das Hype-Thema maschinelles Lernen geht – oder auch „künstliche Intelligenz", wenn man das Buzzword vorzieht. Im April 2018 unterzeichneten 25 Mitgliedstaaten die „Declaration of Cooperation on Artificial Intelligence (AI)"[47] und damit das Ziel, bei der Entwicklung einer gesamteuropäischen Strategie zusammenzuarbeiten. Danach ging es Schlag auf Schlag. Zwei Wochen später veröffentlichte die Europäische Kommission eine entsprechende Kommunikation. Die drei Ziele: Die Wettbewerbsfähigkeit der EU auf dem Feld mit Investitionen in Milliardenhöhe über die nächsten zehn Jahre fördern[48], die Veränderungen auf dem Arbeitsmarkt vorbereiten und eigene ethische Standards für den Einsatz von maschinellen Entscheidungen entwickeln.

Um diese Leitlinien zu schreiben, nahm in Juni 2018 eine Gruppe von 52 unabhängigen ExpertInnen aus Unternehmen, Wissenschaft und Zivilgesellschaft ihre Arbeit auf, die „High Level Expert Group on AI". Knapp ein dreiviertel Jahr später stellte sie tatsächlich Richtlinien für „vertrauenswürdige KI" vor[49]. Im Gremium sitzen allerdings überdurchschnittlich viele VertreterInnen der Industrie. Das wenig überraschende Ergebnis: Die Richtlinien sind nicht bindend und sehen auch wenig Bedarf, Probleme wie den Schutz von Daten, die fehlende Nachvollziehbarkeit von Entscheidungen oder Diskriminierung durch Algorithmen weiter zu regulieren. Klare Formulierungen wie „nicht verhandelbar" oder „rote Linien" wurden durch die Lobbyarbeit der Industrie entschärft.

Im Juni 2019 soll die Gruppe ihre zweite Hausaufgabe abliefern: die konkreten Empfehlungen für eine Investitionsstrategie der EU und Regulierung. Es bleibt also spannend. Egal wie diese Empfehlungen allerdings ausfallen: Bis die Riesenmaschine EU tatsächlich anwendbare Gesetze ausspuckt, die den Einsatz solcher Systeme im Alltag ihrer BürgerInnen regeln, werden mindestens noch fünf Jahre vergehen, schätzen ExpertInnen.

Etwas mehr Schutz für Hinweisgeber

Die Europäische Union arbeitete zuletzt an gleich zwei neue Richtlinien mit erheblichen Auswirkungen auf Whistleblower. Während die Richtlinie zum Schutz von Geschäftsgeheimnissen potentiell eine Bedrohung für Hinweisgeber darstellt, sollte die Whistleblower-Richtlinie erstmals europaweit einheitlichen Schutz für Menschen garantieren, die auf Missstände in Unternehmen hinweisen.

In beiden Fällen gab das Bundesjustizministerium von Katarina Barley eine unrühmliche Figur ab. So versuchte es bei der Umsetzung der Geschäftsgeheimnis-Richtlinie in deutsches Recht erfolglos[50], Ausnahmen für Journalisten und Whistleblower zu verhindern. Bei der Erstellung der Whistleblower-Richtlinie drängte es ebenso erfolglos[51] darauf, Hinweisgebern den Gang an die Öffentlichkeit zu versperren. Letztlich musste sich die Bundesregierung in Verhandlungen dem Europäischen Parlament geschlagen geben, das erstmals eine umfassende Regelung für Whistleblower[52] durchsetzen konnte. In den kommenden zwei Jahren muss die Richtlinie in deutsches Recht überführt werden.

Lobbying und Desinformation

Weiterhin eine Baustelle ist das Thema Lobbytransparenz: Das EU-Parlament gab sich zuletzt neue Regeln[53]: Abgeordnete, die als Berichterstatter Gesetzentwürfe vorlegen oder Ausschüsse leiten, müssen künftig Termine mit Lobbyisten offenlegen. Eine solche Vorschrift gibt es bereits für Spitzenbeamte der EU-Kommission. Doch Gespräche für ein gemeinsames Lobbyregister

aller drei EU-Institutionen – Rat, Parlament und Kommission – scheiterten aber kurz vor der Wahl[54]. Dieses sollte eigentlich alle Treffen von Diplomaten, Beamten und Abgeordneten mit Lobbyisten transparent machen.

Ein politisch heißes Eisen bleibt auch die Frage, wie Europa mit dem Thema Desinformation im Netz umgehen soll (hier unser Explainer zum Thema[55]). Die EU-Kommission drängte die großen Internetplattformen Facebook, Youtube und Twitter in einen freiwilligen Verhaltenskodex. Die Selbstverpflichtung soll sicherstellen, dass die Plattformen die Verbreitung von Falschnachrichten bremsen und sicherstellen, dass bezahlte politische Werbung nicht zur Manipulation von Wählerinnen und Wählern genutzt werden kann.

Die Bilanz der Transparenzbemühungen von Google, Facebook und Co. ist aber bestenfalls gemischt. Die Archive politischer Werbung der beiden großen Plattformen erhalten etwa von den Experten von Mozilla nur mittelmäßige Zensuren[56]. Ein Beispiel kurz vor der Wahl[57] macht zudem deutlich, dass manipulative politische Werbung immer noch zu leicht Platz etwa auf der Werbeplattform von Facebook findet. Immerhin: Es dürfte auch auf den Druck der EU zurückzuführen sein, dass Facebook jetzt Informationen darüber veröffentlicht, wieviel Geld politische Akteure für Werbung in den Sozialen Netzwerken ausgeben[58].

Fazit: Geht wählen, es war nie wichtiger!

Die großen Debatten der Netzpolitik finden auf EU-Ebene statt: Schlüsselthemen der vergangenen Jahre, von Netzneutralität über Datenschutz bis Urheberrecht, wurden in Brüssel und Straßburg verhandelt.

Die kommenden Jahre werden entscheidend sein bei der Frage, in welcher digitalen Gesellschaft wir leben wollen. Es wird große

Die Autoren

Alexander Fanta ist EU-Korrespondent für *netzpolitik.org* in Brüssel. Er berichtet über Datenschutz, Urheberrecht und alles Digitale. 2017 beschäftigte er sich als Stipendiat am *Reuters-Institut für Journalismusforschung* in Oxford mit automatisiertem Journalismus. Davor arbeitete Alexander für die österreichische Nachrichtenagentur *APA*. Er ist unter *alexander.fanta ett Netzpolitik.org* (PGP[60]) und unter *@FantaAlexx* erreichbar.

Ingo Dachwitz ist Medien- und Kommunikationswissenschaftler, Redakteur bei *netzpolitik.org* und Mitglied beim Verein *Digitale Gesellschaft*. Er schreibt und spricht über Datenkapitalismus, Datenschutz und den digitalen Strukturwandel der Öffentlichkeit. Ingo gibt Workshops für junge und ältere Menschen in digitaler Selbstverteidigung und lehrt im internationalen Studiengang „*Digital Media*“[61] zur politischen Ökonomie digitaler Medien. Gelegentlich moderiert er Veranstaltungen und Diskussionen, etwa auf der *re:publica* oder beim *Netzpolitischen Abend* in Berlin. Ingo ist Mitglied der sozialethischen Kammer der EKD und versucht, auch die Evangelische Kirche mit dem digitalen Zeitalter vertraut zu machen. Kontakt: Ingo ist per Mail an *ingo | ett | netzpolitik.org* (PGP-Key[62]) erreichbar und als *@roofjoke* auf Twitter unterwegs.

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 +49-30-92105-9861 oder *tomas@netzpolitik.org* (PGP-Key[63]) erreichbar und twittert mal mehr, mal weniger unter *@tomas_np*

Chris Köver schreibt über Datenschutz, Künstliche Intelligenz, Netzkultur und soziale Bewegungen. Sie hat als Autorin für *Die Zeit*, *De:bug* und *Spiegel Online* gearbeitet. Von 2008 bis 2014 war sie Chefredakteurin des *Missy Magazine*[64], später arbeitete sie in der Redaktion von *WIRED Germany*. Seit Sommer 2018 ist sie Redakteurin bei *Netzpolitik.org*. Kontakt: E-Mail[65], OpenPGP[66], Twitter[67].

Arne Semsrott arbeitet für die Open Knowledge Foundation Deutschland und betreut dort das Portal zur *Informationsfreiheit FragDenStaat.de*. Twitter: *@fragdenstaat* E-Mail (PGP[68]): *arne(at)netzpolitik.org.*

Matthias Monroy ist Wissensarbeiter, Aktivist und Mitglied der Redaktion der Zeitschrift *Bürgerrechte & Polizei/CILIP*[69]. In Teilzeit Mitarbeiter des MdB Andrej Hunko. Publiziert in linken Zeitungen, Zeitschriften und Online-Medien, bei *Telepolis*, *Netzpolitik* und in Freien Radios. Alle Texte und Interviews unter *digit.so36.net*, auf englisch *digit.site36.net*, auf Twitter *@matthimon*. Viel zu selten auf der Straße (dafür im Internet) gegen Faschismus, Rassismus, Sexismus, Antisemitismus. Kein Anhänger von Verschwörungstheorien jeglicher Couleur. Freut sich nicht über Kommentare von AnhängerInnen der genannten Phänomene. Benutzt das (altmodische) Binnen-I trotz Gepolter nervtötender Maskulisten.

Markus Beckedahl ist Gründer und Chefredakteur von *netzpolitik.org*. Er ist Partner bei *newthinking communications GmbH*[70], Gründer der *re:publica*[71] und Mitglied im Medienrat der *Landesmedienanstalt Berlin-Brandenburg*. In der Zeit vor netzpolitik.org war er mal bei den Grünen aktiv. **Kontakt:** Mail: *markus (ett) netzpolitik.org* / Telefon: +49-30-92105-986 (zu Arbeitszeiten) – Facebook: Profil[72]; Twitter: *@netzpolitik*; Instagram: *@netzpolitik*; Amazon: Die Wunschliste von Markus[73]

Kämpfe um Themen wie eine mögliche Aufweichung des Providerprivilegs[59] geben, die das offene Netz gefährden – aber vielleicht auch stabilisieren könnten. Wir werden über mögliche Wege reden, die Macht der großen Plattformen zu begrenzen, ohne neuen Mitbewerbern Steine in den Weg zu legen.

Wenn wir weiter einen Rechtsruck in der EU erleben und das EU-Parlament in diese Richtung abdriften sollte, dann wird es schwieriger werden, sich für eine grundrechts- und gemeinwohlorientierte Netzpolitik einzusetzen. Dann werden wir uns gegen noch mehr Überwachungsgesetze engagieren müssen.

Bis heute hat das EU-Parlament keine ausreichende Mitsprachemöglichkeit in den EU-Institutionen, etwa kein Vorschlagsrecht für neue Gesetze. Dennoch können engagierte Abgeordnete im Zusammenspiel mit der digitalen Zivilgesellschaft viel erreichen – viel mehr als einzelne Abgeordnete im Bundestag. Das haben Jan Philipp Albrecht (Bündnis 90/Die Grünen) und Julia Reda (Ex-Piratin in der Grünen-Fraktion) eindrucksvoll bei den Themen Datenschutz und Urheberrecht gezeigt. Ohne ihren Einsatz sähe es bei den Themen schlecht beziehungsweise noch schlechter aus. Dass es auch anders laufen kann, zeigen eindrucksvolle Beispiele wie Günther Oettinger, der allzu industriefreundliche deutsche EU-Kommissar, und Axel Voss, der CDU-Parlamentarier mit dem direkten Draht zur Verlagsbranche.

Deshalb ist aus netzpolitischer Sicht die EU-Wahl die relevanteste Wahlentscheidung. Geht wählen, es war nie wichtiger!

Anmerkungen

1 *https://ec.europa.eu/commission/priorities/digital-single-market_de*
2 *https://netzpolitik.org/2019/copyfail-eu-parlament-beschliesst-uploadfilter/*
3 *https://netzpolitik.org/2019/urheberrechtsreform-was-in-den-letzten-drei-jahren-geschah/*
4 *https://netzpolitik.org/2019/chance-verpasst-dieses-urheberrecht-bleibt-in-der-vergangenheit-stecken/*
5 *https://netzpolitik.org/2019/schnell-schnell-so-geht-es-mit-den-uploadfiltern-gegen-propaganda-weiter/*
6 *https://netzpolitik.org/2019/plattformen-die-zukunft-von-notice-takedown-in-europa/*
7 *https://www.gutjahr.biz/2013/02/lobbyplag/*
8 *https://www.heise.de/newsticker/meldung/Versprechen-und-Drohungen-Facebooks-Lobby-Schlacht-gegen-die-DSGVO-4325271.html*
9 *https://netzpolitik.org/2015/wie-einflussnahme-funktioniert-lobby-mails-zum-durchklicken/*
10 *https://netzpolitik.org/2018/datenschutzgrundverunsicherung-danke-merkel/*
11 *https://netzpolitik.org/2018/abmahnungen-und-der-datenschutz-den-deutschen-sonderweg-beenden/*
12 *https://de.wikipedia.org/wiki/EU-US_Privacy_Shield*
13 *https://netzpolitik.org/2015/europaeischer-gerichtshof-safe-harbor-ist-ungueltig-schluss-mit-der-blauaeugigen-datenuebertragung-in-die-usa/*
14 *https://netzpolitik.org/2017/sechs-gruende-warum-die-totlangweilig-klingende-eprivacy-verordnung-fuer-dich-wichtig-ist/*
15 *https://netzpolitik.org/der-facebook-cambridge-analytica-datenskandal/*
16 *https://netzpolitik.org/2018/schutz-gegen-tracking-unerwuenscht-oesterreich-verschiebt-eprivacy-reform-auf-den-st-nimmerleinstag/*
17 *https://netzpolitik.org/2017/eprivacy-datenschutzbeauftragte-kritisiert-einseitige-studie-des-wirtschaftsministeriums/*
18 *https://netzpolitik.org/2019/eu-staaten-vertroedeln-den-datenschutz-bis-nach-der-europawahl/*
19 *http://europa.eu/rapid/press-release_IP-17-1784_de.htm*
20 *http://europa.eu/rapid/press-release_IP-18-4581_de.htm*
21 *http://europa.eu/rapid/press-release_IP-19-1770_de.htm*
22 *http://europa.eu/rapid/press-release_IP-16-2923_de.htm*
23 *https://www.reuters.com/article/eu-google-antitrust-vestager/update-1-after-record-google-fine-eus-vestager-says-she-likes-the-us-idUSL8N1UE3X5*
24 *https://netzpolitik.org/2018/den-datenfischern-die-netze-kappen-ideen-gegen-die-marktmacht-der-plattformen/*
25 *https://netzpolitik.org/2018/handelskrieg-wie-die-industrie-gegen-die-digitalsteuer-der-eu-mobil-macht/*
26 *https://www.spiegel.de/wirtschaft/soziales/digitalsteuer-eu-gibt-plaene-fuer-gemeinsame-abgabe-auf-a-1257478.html*
27 *https://netzpolitik.org/2013/neelie-kroes-will-keine-netzneutralitat-sichern-sondern-bereitet-ihre-beerdigung-vor/*
28 *https://www.handelsblatt.com/today/politics/internet-intentions-spurring-europes-digital-development/23614536.html*
29 *https://netzpolitik.org/2016/fast-500-000-stimmen-fuer-netzneutralitaet-bei-eu-konsultation/*
30 *https://netzpolitik.org/2016/europa-sichert-die-netzneutralitaet-das-bedeuten-die-regeln-im-alltag/*
31 *https://netzpolitik.org/2018/netzneutralitaet-und-zero-rating-vom-schlupfloch-zum-scheunentor/*
32 *https://netzpolitik.org/2019/katarina-barley-stellt-sich-gegen-netzneutralitaet/*
33 *https://netzpolitik.org/2017/die-usa-schaffen-ihre-netzneutralitaet-ab-was-alles-dahintersteckt/*
34 *https://twitter.com/ansip_eu/status/941602056137256960?lang=en*
35 *https://www.euractiv.de/section/digitale-agenda/news/gleiches-ziel-andere-ansaetze-netzneutralitaet-in-der-eu-und-den-usa/*
36 *https://netzpolitik.org/2017/das-ende-der-roaming-gebuehren-erfolgsgeschichte-mit-luecken/*
37 *https://ec.europa.eu/home-affairs/news/20190514_security-union-eu-closes-gaps-between-information-systems-security-borders-migration-management_en*
38 *https://netzpolitik.org/2019/eu-legt-biometrische-datentoepfe-zusammen-jetzt-droht-der-abfrage-tsunami/*
39 *http://europa.eu/rapid/press-release_IP-18-3343_de.htm*
40 *https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_de*
41 *https://netzpolitik.org/2018/elektronische-beweismittel-eu-staaten-drohen-online-diensten-mit-hohen-strafen/*
42 *https://www.eff.org/de/deeplinks/2018/02/cloud-act-dangerous-expansion-police-snooping-cross-border-data*
43 *https://en.wikipedia.org/wiki/Convention_on_Cybercrime*
44 *https://netzpolitik.org/2019/speicherpflicht-bald-fingerabdruecke-in-allen-personalausweisen/*
45 *https://netzpolitik.org/2016/stapeln-schichten-rastern-die-umsetzung-der-eu-richtlinie-ueber-die-verwendung-von-fluggastdaten/*
46 *https://netzpolitik.org/2019/fahrzeug-blackbox-wenn-dein-auto-gegen-dich-aussagt/*
47 *https://ec.europa.eu/digital-single-market/en/news/eu-member-states-sign-cooperate-artificial-intelligence*
48 *https://ec.europa.eu/digital-single-market/en/news/factsheet-artificial-intelligence-europe*

49 https://netzpolitik.org/2019/keine-roten-linien-industrie-entschaerft-ethik-leitlinien-fuer-kuenstliche-intelligenz/
50 https://netzpolitik.org/2018/wir-veroeffentlichen-den-gesetzentwurf-zu-geschaeftsgeheimnissen-fehlender-schutz-fuer-whistleblower/
51 https://netzpolitik.org/2019/barley-hat-kein-herz-fuer-whistleblower-justizministerium-blockiert-eu-gesetz/
52 https://netzpolitik.org/2019/eu-verhandler-einigen-sich-auf-mehr-schutz-fuer-whistleblower/
53 https://netzpolitik.org/2019/lobbyregister-eu-parlament-stimmt-ueberraschend-fuer-mehr-transparenz/
54 https://euobserver.com/institutional/144599
55 https://netzpolitik.org/2019/was-die-eu-meint-wenn-sie-ueber-desinformation-spricht/
56 https://blog.mozilla.org/blog/2019/05/10/googles-ad-api-is-better-than-facebooks-but/
57 https://www.bitsoffreedom.nl/2019/05/21/facebook-lies-to-dutch-parliament-about-election-manipulation/
58 https://netzpolitik.org/2019/zahlen-bitte-so-viel-geben-deutsche-parteien-fuer-werbung-auf-facebook-aus/
59 https://de.wikipedia.org/wiki/Providerprivileg
60 http://pool.sks-keyservers.net/pks/lookup?op=get&search=0x2271FE6D4CD84C62
61 https://www.leuphana.de/college/bachelor/digital-media.html
62 https://pgp.mit.edu/pks/lookup?op=get&search=0x05550760A5E4E814
63 https://pgp.mit.edu/pks/lookup?op=get&search=0x745121858AE13AED
64 http://www.missy-magazine.de/
65 mailto:chris@netzpolitik.org
66 https://sks-keyservers.net/pks/lookup?op=get&search=0x5E598DD0D37B9F71A88DD92233D38859243016F9
67 http://www.twitter.com/ckoever
68 https://pgp.mit.edu/pks/lookup?op=get&search=0x6465557231B9172C
69 http://www.cilip.de/
70 http://newthinking.de/
71 http://re-publica.de/
72 https://www.facebook.com/beckedahl
73 http://www.amazon.de/gp/registry/wishlist/279FWSUX7VB9

Ingo Dachwitz, Markus Reuter

Warum Künstliche Intelligenz Facebooks Moderationsprobleme nicht lösen kann, ohne neue zu schaffen

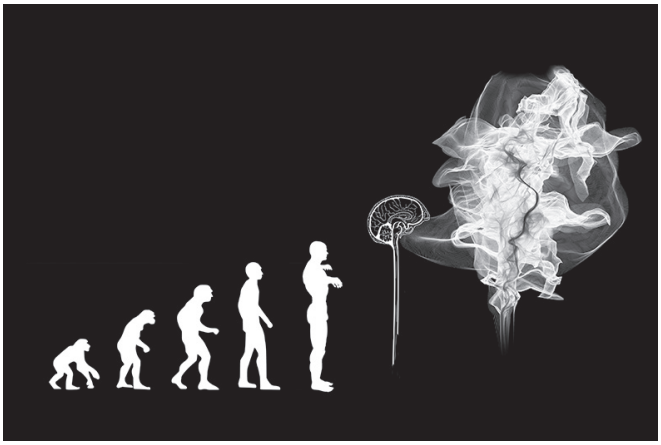
Der Datenkonzern Facebook setzt bei der Moderation von Inhalten zunehmend auf Automatisierung. Eine Quelle erklärt uns erstmals, wie sich die Maschinen auf die Moderationsarbeit auswirken. Auch wenn am Ende heute immer noch Menschen entscheiden: Die automatisierte Inhaltserkennung verändert die digitale Öffentlichkeit grundlegend.

„Auf einmal waren da diese merkwürdigen Tickets." Mika* arbeitet in Essen beim Dienstleister CCC und moderiert dort im Auftrag von Facebook Posts, Videos und Bilder[1], die gegen die Regeln des Konzerns verstoßen könnten. Schon in normalen Wochen bekommen die Moderator:innen viele Meldungen vorgelegt, die bei ihnen Stirnrunzeln auslösen. An diesem Tag wirkten die Posts besonders wahllos zusammengewürfelt: Oft war an ihnen überhaupt nichts auszusetzen, außer dass ein bestimmtes Wort doppeldeutig war. „Proactive Queue" heißt Ticket-Warteschlage, in der diese merkwürdigen Inhalte zur Moderation vorgelegt wurden.

Es dauerte eine Weile, bis Mika und den KollegInnen dämmerte, womit sie es zu tun hatten: Proaktiv – das heißt, dass Facebooks Software selbst Inhalte sucht und zur Löschung vorschlägt, die sie für verdächtig hält. Heute setzt der Weltkonzern im großen Stil auf diese automatisierte Erkennung unerwünschter Inhalte. Es ist ein qualitativer Sprung: Lange wurden die Beiträge, über die die Moderator:innen zu entscheiden hatten, nur von Menschen gemeldet. Sie markieren etwa ein Bild als anstößig, gewalttätig oder obszön, so dass es als Ticket in einem Kanal landet und auf dem Bildschirm von Content-ModeratorInnen wie Mika aufschlägt.

Künstliche Intelligenz soll es richten

Wann immer Facebook-Chef Mark Zuckerberg bei den Anhörungen im US-Senat im vergangenen Jahr auf Probleme mit Hetze und anderen unerwünschten Inhalten auf seiner Plattform angesprochen wurde, hatte er für die Politik eine einfache



Evolution wohin?

Antwort parat: „AI will fix this", Künstliche Intelligenz wird es richten. Doch immer mehr ExpertInnen melden Zweifel daran an[2], dass Automatisierung Facebooks Probleme tatsächlich lösen kann. Gleichzeitig können wir beobachten, wie die automatische Vormoderation die digitale Öffentlichkeit schon heute verändert.

Mehr als zwei Milliarden Menschen nutzen laut Unternehmensangaben die von Facebook bereitgestellten Dienste für ihre Kommunikation. Sie diskutieren, streiten, lieben, hassen auf den Plattform des Konzerns. Man findet auf Facebook alles, was das Menschsein ausmacht. Auch Tod und Gewalt in allen Variationen. „Es gibt nichts, was nicht geteilt wird", erzählt Mika lakonisch. Damit Videos von Vergewaltigungen und Enthauptungen

nicht online bleiben, beschäftigt Facebook über Drittfirmen ein Heer von ModeratorInnen – und ein Heer von Maschinen.

Nur für den Dienstgebrauch: Content-Moderation als Staatsgeheimnis

Wie genau das System funktioniert, soll die Öffentlichkeit nicht erfahren. Der Konzern zieht seine Maßnahmen für die Content-Moderation auf wie ein Staatsgeheimnis, ModeratorInnen müssen Geheimhaltungsverträge unterschreiben. Und gerade beim Thema KI lässt sich Mark Zuckerberg ungern in die Karten schauen.

Bekannt ist, dass der Konzern neben digitalen Fingerabdrücken zur automatischen Wiedererkennung bereits gesperrter Inhalte[3] auf maschinelles Lernen setzt. Ein algorithmisches System erkennt hierbei Muster in Trainingsdaten und trifft auf Basis der daraus abgeleiteten Regeln Prognosen zur Bewertung neuer Fälle. Sehr vereinfacht gesagt heißt das: Wenn Post X und Post Y gegen die Gemeinschaftsstandards verstoßen haben, dann tut es Post Z, der ähnliche Eigenschaften aufweist wie X und Y, mit hoher Wahrscheinlichkeit auch.

Durch die schiere Menge zur Verfügung stehender Daten und die gestiegenen Rechenkapazitäten hat diese Form der „Künstlichen Intelligenz" in den vergangenen Jahren enorme Fortschritte gemacht. Sie hilft bei der Diagnose von Krebs, ermöglicht Autos, die fast autonom fahren und Sprachassistenten, die uns zehn Minuten eher wecken, wenn auf dem Weg zur Arbeit Stau herrscht. Doch bei menschlichen Sprache und der komplexen Abwägung, welche auf einer Plattform legitim sind und welche nicht, stößt die Technologie an ihre Grenzen.

Kultur ist nicht maschinenlesbar

Die merkwürdigen Meldungen, über die Mika und KollegInnen sich wunderten, kamen dadurch zustande, dass das System sich auf bestimmte Schlagworte gestürzt hat, die häufig problematisch waren. In einem anderen Kontext, etwa eine in einen Scherz oder Satire eingebette Beleidung, war ihre Verwendung jedoch vollkommen unproblematisch. „Am Anfang kam da ziemlich viel Schwachsinn", sagt Mika über die Proactive Queue. Mit der Zeit sei das System dann besser geworden. „Wir trainieren die KI, indem wir ihre Vorschläge als richtig oder falsch bewerten." Anfangs häufig wiederkehrende Fehlalarme seien nach einer Weile nicht mehr passiert. Dafür seien neue Fehler aufgetaucht.

Das Problem ist, dass die Unterscheidung dessen, was erlaubt und was verboten ist, in liberalen Gesellschaften eine komplexe Angelegenheit ist. Oft entscheidet der Kontext – und der ist für Maschinen schwer zu erfassen. Meinungsfreiheit ist ein relationales und fluides soziales Konstrukt, dass sich nicht in Formeln übersetzen lässt. Aus diesem Grund bekommen menschliche Moderator:innen bei der Bearbeitung von gemeldeten Chatnachrichten Mika zufolge nicht nur die eine Nachricht, sondern auch einen Ausschnitt des Nachrichtenverlaufs zu sehen.

Bei Bildern funktioniert die Automatisierung besser: „Pornographie erkennt die Software inzwischen ziemlich zuverlässig", erzählt Mika. Etwa 96 Prozent der wegen Nacktheit wegmoderierten Bilder[4] sind laut Facebook-Angaben durch „Erkennungstechnologie" entdeckt worden. Wie fehleranfällig KI aber auch in diesem Bereich ist, verdeutlicht der Versuch der Blogplattform Tumblr, pornographische Inhalte automatisiert löschen zu lassen. Neben harmlosen Comics[5] sperrte das System auch ein Foto des ehemaligen US-Vizepräsidenten Joe Biden[6]. Viel hängt davon ab, wie gut die KI trainiert ist – dass sie jemals zuverlässig legitime und illegtime Inhalte auseinanderhalten kann, darf bezweifelt werden.

Facebook selbst pflegt neben der Geschichte von KI als Rettung deshalb ein zweites Narrativ, das inzwischen noch häufiger betont wird: Am Ende würden alle relevanten Entscheidungen von Menschen getroffen. Die Software mache zwar Vorschläge zur Moderation, aber die Entscheidungshoheit liege bei den Moderator:innen. Niemand soll den Eindruck bekommen, Maschinen würden über das hohe Gut der Meinungsfreiheit entscheiden.

Technische Lösungen für soziale Probleme

Doch selbst, wenn jede Moderationsentscheidung am Ende durch einen Menschen geprüft wird, hat die Ausbreitung der Maschinen in der Content Moderation einen profunden Einfluss auf die digitale Öffentlichkeit. Er bedeutet nicht weniger als die Umkehr eines der Grundgesetze des Internets: Bisher durften auch unerwünschte Inhalte auf Plattformen so lange online bleiben, bis sie von irgendwem beim Betreiber einer Seite gemeldet werden. Auch für illegale Inhalte tragen Hoster erst dann eine Verantwortung, wenn sie darauf hingewiesen wurden und den Post trotzdem nicht löschen.

Dieses „Notice and Takedown"[7] genannte Prinzip ist in der EU in der E-Commerce-Richtlinie verankert und konstituierend für ein freies Internet. Bei Plattformbetreibern wie Facebook, Youtube und Twitter hat es lange Zeit zu Verantwortungslosigkeit im Umgang mit verletzenden Inhalten geführt. Aber es hat auch einen Teil der anarchischen Freiheit früher Internettage in die Welt der Plattformmonopole gerettet: Selbst in den Gruppen und Chats von Facebook war Raum für Inhalte, die gegen Regeln wie das rigide Nacktheitsverbot[8] verstoßen.

Mit dem großflächigen Einsatz von Erkennungssoftware kommt Facebook der EU-Kommission zuvor, die derzeit darauf drängt, automatische Erkennung auszuweiten. Die hochumstrittene neue Urheberrechtsrichtlinie[9] wird zur Folge haben, dass Plattformen Inhalte proaktiv und vor deren Veröffentlichung auf Urheberrechtsverletzungen untersuchen. In Anbetracht der täglich von Nutzer:innen veröffentlichten Inhalte ist dies nur durch automatische Systeme möglich. Auch für „terroristische Inhalte"[10] will die EU ähnliche Regeln. Was als verboten eingestuft wird, soll nicht nur erkannt werden, sondern gar nicht mehr gepostet werden dürfen. Trotz der bekannten Probleme bei der automatisierten Erkennung des kulturellen Kontextes von Inhalten setzt die EU auf technische Lösungen für soziale Probleme[11].

Wird diese Logik jedoch ausgeweitet, werden die unerwünschten Nebeneffekte[12] zunehmen. Immer wieder werden Vorwürfe laut, das System schieße über das Ziel hinaus. Die Nichtregie-

rungsorganisation *Reporter Ohne Grenzen* etwa machte 2016 auf den Fall des französischen Journalisten und Terrorexperten David Thomson aufmerksam. Sein Account wurde gesperrt, weil auf einem mehrere Jahre alten Bild die Flagge der Terrorgruppe Islamischer Staat/Daesh zu sehen war[13]. Dass ein Mensch sich an dem von Thomson eingeordneten und damals noch nicht verbotenen Symbol störte, ist eher unwahrscheinlich. Stattdessen dürfte der Post in den Schleppnetzen von Facebooks Algorithmus gelandet sein.

Welche Öffentlichkeit wollen wir?

Tatsächlich könnte die automatische Inhalteerkennung sogar noch ausgeweitet werden: In einer vielbeachteten Petition fordert die Kampagnenorganisation Avaaz Mark Zuckerberg auf, automatische Filter auch in den bisher verschlüsselten WhatsApp-Chats zu installieren[14]. Vor dem Hintergrund des von Falschnachrichten geprägten brasilianischen Präsidentschaftswahlkampfes soll dies gegen Desinformation helfen.

Kann Facebook also sein Moderationsprobleme mit Künstlicher Intelligenz lösen? Nur zu einem hohen Preis. Wenn wir über die Zukunft der digitalen Öffentlichkeit nachdenken, sollten wir deshalb gut überlegen, welche Bereiche wir tatsächlich an Maschinen auslagern wollen. Mark Zuckerberg sagt, seine Systeme seien in fünf bis zehn Jahren soweit[15], jegliche Inhalte sauber zu moderieren. Auch Mika selbst rechnet fest damit, auf Kurz oder Lang von der Software ersetzt zu werden: „Irgendwann sind wir überflüssig."

Über diese Recherche und die Quellen:

Unser Wissen über die Organisation des Löschzentrums in Essen beruht auf einem mehrstündigen Gespräch von drei Redakteuren von netzpolitik.org mit einer Quelle bei Competence Call Center, die wir im Text geschlechterneutral Mika nennen. Wir können und wollen die Quelle, die wir für glaubwürdig halten, aus Gründen des Informantenschutzes nicht näher beschreiben. Wir sind uns der Probleme und des Risikos bewusst, dass wir uns in Teilen dieser Recherche nur auf eine Quelle stützen können. Deswegen haben wir weite Teile des Artikels durch andere Quellen, auch von anderen Facebook-Dienstleistern verifizieren und bestätigen lassen. Durch diese Quellen können wir heute sagen, dass bei allen Dienstleistern sehr ähnliche oder gar gleiche Systeme eingesetzt werden. Weite Teile dieser Recherche hat außerdem Facebook uns gegenüber bestätigt, die Dienstleister selbst gaben kein Statement ab.

Anmerkungen

1 *https://netzpolitik.org/2019/warum-kuenstliche-intelligenz-facebooks-moderationsprobleme-nicht-loesen-kann-ohne-neue-zu-schaffen/srt*
2 *https://www.theverge.com/2019/2/27/18242724/facebook-moderation-ai-artificial-intelligence-platforms*
3 *https://netzpolitik.org/2017/facebook-twitter-co-upload-filter-gegen-terrorismus-und-extremismus-gestartet/*
4 *https://transparency.facebook.com/community-standards-enforcement#adult-nudity-and-sexual-activity*
5 *https://www.wired.com/story/tumblr-porn-ai-adult-content/*
6 *https://twitter.com/search?f=tweets&q=%23toosexyfortumblr%20joe%20biden&src=typd*
7 *https://netzpolitik.org/2019/plattformen-die-zukunft-von-notice-takedown-in-europa/*
8 *https://netzpolitik.org/2018/facebook-verbannt-mit-neuer-regel-allen-sex-von-seiner-plattform/*
9 *https://netzpolitik.org/tag/eu-urheberrechtsreform/*
10 *https://netzpolitik.org/tag/terreg/*
11 *https://netzpolitik.org/2019/christchurch-es-gibt-keine-technische-loesung-fuer-rechten-terrorismus/*
12 *https://netzpolitik.org/2019/uploadfilter-eine-geschichte-voller-fails/*
13 *https://www.reporter-ohne-grenzen.de/pressemitteilungen/meldung/facebook-muss-sperrung-von-konten-erklaeren/*
14 *https://secure.avaaz.org/campaign/en/wa_destroys_democracy_30/*
15 *https://www.washingtonpost.com/news/the-switch/wp/2018/04/11/ai-will-solve-facebooks-most-vexing-problems-mark-zuckerberg-says-just-dont-ask-when-or-how/*
16 *https://www.leuphana.de/college/bachelor/digital-media.html*
17 *https://pgp.mit.edu/pks/lookup?op=get&search=0x05550760A5E4E814*
18 *http://pgp.mit.edu/pks/lookup?op=get&search=0xB8020A34EF5B7E17*

Ingo Dachwitz und Markus Reuter

Ingo Dachwitz ist Medien- und Kommunikationswissenschaftler, Redakteur bei *netzpolitik.org* und Mitglied beim Verein *Digitale Gesellschaft*. Er schreibt und spricht über Datenkapitalismus, Datenschutz und den digitalen Strukturwandel der Öffentlichkeit. Ingo gibt Workshops für junge und ältere Menschen in digitaler Selbstverteidigung und lehrt im internationalen Studiengang „*Digital Media*"[16] zur politischen Ökonomie digitaler Medien. Gelegentlich moderiert er Veranstaltungen und Diskussionen, etwa auf der *re:publica* oder beim *Netzpolitischen Abend* in Berlin. Ingo ist Mitglied der sozialethischen Kammer der EKD und versucht, auch die Evangelische Kirche mit dem digitalen Zeitalter vertraut zu machen. Kontakt: Ingo ist per Mail an *ingo | ett | netzpolitik.org* (PGP-Key[17]) erreichbar und als *@roofjoke* auf Twitter unterwegs.

Markus Reuter beschäftigt sich mit den Themen Digital Rights, Hate Speech & Zensur, Fake News & Social Bots, 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* (OpenPGP[18]) und auf Twitter unter *@markusreuter_*.

Markus Beckedahl

Europawahl: Dieser Wahlkampf wurde im Internet entschieden

Es war nicht nur der Rezo-Effekt: Erstmals wurde ein EU-Wahlkampf maßgeblich im Netz entschieden. Das ist vor allem der Verdienst der Jungen. Sie brachten Online- und Offline-Protest zusammen und setzten so ihre Themen Klimaschutz und Urheberrecht auf die Agenda. Das wird die politischen Spielregeln dauerhaft verändern.

Am Ende wurde es doch noch ein spannender Europawahlkampf. Er wurde nur anders als die vielen Hoodie-tragenden Politiker:innen sich erhofft hatten. Wir haben den ersten großen Wahlkampf gesehen, bei dem das Netz eine bestimmende Rolle übernommen hat. Die Zeiten, in denen Wahlkampf ausschließlich mit Zeitung und Fernsehen gemacht wurde, sind damit endgültig vorbei.

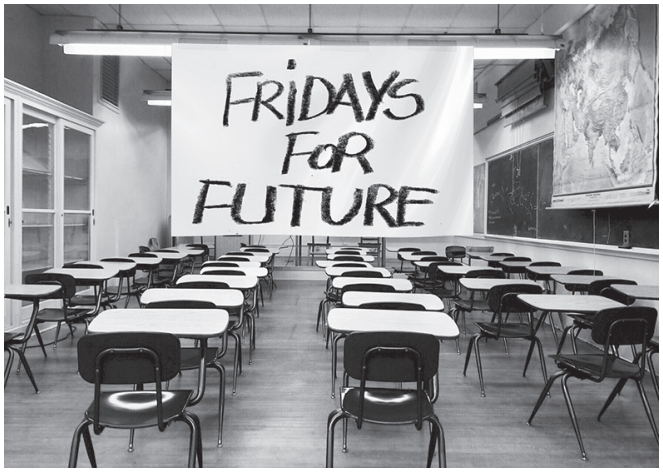
Das konnte man spätestens in der vergangenen Woche beobachten, als das Video „Die Zerstörung der CDU“[1] des Youtubers Rezo millionenfach geklickt und geteilt wurde[2]. Tagelang zeigte die CDU-Spitze, dass sie vollkommen unfähig war, darauf eine Antwort zu finden und dass sich etwas massiv in unserer Gesellschaft verschoben hat. Während in diesen Tagen bei den Sozialdemokraten noch etwas Hoffnung aufkam, gerade durch das schlechte Image der CDU/CSU noch Punkte bei den Jungen zu sammeln, wurde diese Hoffnung dann am Freitagnachmittag beerdigt. Mehr als 70 YoutuberInnen riefen gemeinsam3 in einem Video-Statement dazu auf, weder CDU/CSU noch SPD oder AfD zu wählen.

Von der Urheberrechtsreform zu den „Fridays for Future“-Protesten

Vorboten dieser Entwicklung sah man bereits im März, als die Auseinandersetzung rund um die EU-Urheberrechtsreform im Netz eskalierte[4]. Diverse PolitikerInnen von CDU/CSU bezeichneten die Protestierenden, meist junge Menschen, pauschal als gekaufte Demonstranten, Social Bots und von Konzernen instrumentalisierte Falschmeldungsverbreiter. Im Nachhinein eine ziemlich dumme Idee, wie man aus den damals trendigen Hashtags #niewiedercdu ablesen konnte.

Im Rückblick dürfte auch der Union auffallen, dass das Abqualifizieren junger Menschen für ihre legitimen Anliegen eine schlechte Idee war. Das kann man jetzt in zahlreichen Grafiken anschauen[5], die zeigen, dass die Union nur noch bei den Alten vorne liegt.

Und auch das gewohnte Rumgeeier der SPD sorgte nicht für mehr Vertrauen: Erst gegen Uploadfilter sein, dann aber in der



Regierung mitstimmen, obwohl der Koalitionsvertrag diese ausschloss, um dann doch irgendwie dafür und dagegen gleichzeitig zu sein. Also kam #niewiederspd dazu.

Hier zeigte sich schon eine massive Verschiebung in der Wahrnehmung der Realität. LeserInnen der FAZ, in der die Proteste ebenfalls konsequent delegitimiert wurden, lebten in einer anderen Realität als NetzbewohnerInnen. Und hatten wohl eine andere Vorstellung der Gestaltung der Zukunft als die junge Generation.

Ich bin mal gespannt, ob unter Unionspolitiker:innen auch eine Debatte über die Rolle der FAZ als meinungsführendes Medium aufkommen wird, die offensichtlich mit dafür verantwortlich war, dass viele PolitikerInnen die Situation vollkommen falsch einschätzten.

Politikverdrossenheit? Wir erleben eine Re-Politisierung der Zivilgesellschaft

Es war keine überraschende Entwicklung. Bereits in den vergangenen Monaten zeigte sich, dass wir eine neue Politisierung von Teilen der Gesellschaft erleben. Das sah man auf den zahlreichen Großdemonstrationen: den Protesten gegen ausufernde Polizeigesetze mit 40.000 Menschen allein in München, die #Unteilbar-Demo mit 240.000 Demonstrierenden im vergangenen

Markus Beckedahl

Markus Beckedahl ist Gründer und Chefredakteur von *netzpolitik.org*. Er ist Partner bei *newthinking communications GmbH*[6], Gründer der *re:publica*[7] und Mitglied im Medienrat der *Landesmedienanstalt Berlin-Brandenburg*. In der Zeit vor netzpolitik.org war er mal bei den Grünen aktiv. Kontakt: Mail: *markus (ett) netzpolitik.org* / Telefon: +49-30-92105-986 (zu Arbeitszeiten) – Facebook: Profil[8]; Twitter: *@netzpolitik*; Instagram: *@netzpolitik*; Amazon: Die Wunschliste von Markus[9].

Herbst in Berlin, die Proteste gegen die EU-Urheberrechtsreform und Uploadfilter mit über 200.000 Menschen bis zu den regelmäßigen „Fridays for future"-Demonstrationen und Aktionstagen mit etwa 300.000 Teilnehmenden im März und am am vergangenen Freitag.

Die Demonstrant:innen haben dabei wie nie zuvor den Protest auf der Straße mit dem im Netz verbunden. Nicht nur prägten die Memes aus den Sozialen Medien die zahlreichen Demoschilder. Durch Streams, Protestsongs und Nachbesprechungen wurde der Offline-Protest online weitergetragen und verstärkt.

So gelang einer engagierten Zivilgesellschaft das lange scheinbar Unmögliche: das bisher medial und politisch dominierenden Thema Migration durch das wesentlich relevantere Thema Klimarettung abzulösen. Das haben wir vor allem einer jungen Generation zu verdanken, die sich nicht mehr damit abfinden will, dass die Älteren über ihre Zukunft bestimmen. Sie hat es geschafft, das Hauptnarrativ der Populisten endlich von Platz 1 zu verdrängen. Mal schauen, wann das die Redaktionen der Polit-Talkshows im TV mitbekommen.

Davon profitiert haben vor allem die Grünen, die für diese Themen stehen und denen ein Einsatz dafür am ehesten zugetraut wird. In den acht größten Städten Deutschlands liegen Bündnis 90/Die Grünen vorne. Welche Auswirkungen dieses Wahlergebnis auf den Fortbestand der Großen Koalition haben wird, kann man gerade noch nicht absehen.

Interessante Verschiebungen im EU-Parlament

Auf EU-Ebene sehen wir auch spannende Entwicklungen. Die große Furcht vor dieser Wahl war, dass die Nazis und Rechtspopulisten massiv zulegen und zu einem größeren Machtblock werden. Stattdessen sind vor allem Liberale und Grüne als Fraktionen gestärkt, während Konservative und auch Sozialdemokratien verloren haben. Das bedeutet auch, dass die Zeiten einer losen Großen Koalition im EU-Parlament vorbei sind. Aus der

Jetzt gilt's – Demonstration am 2018-10-03 auf dem Münchner Odeonsplatz. Gemeinsamer Aktionstag von #NoPAG und Ausgehetzt mit rund 100 aufrufenden Organisationen gegen Rechtsruck und Polizeigesetz, Foto: Henning Schlottmann – CC BY-SA 4.0

Perspektive von Grundrechten kann sich das positiv auswirken.

Wir leben in spannenden politischen Zeiten. Das war mal anders. Machen wir was draus.

Anmerkungen

1 *https://www.youtube.com/watch?v=4Y1lZQsyuSQ*
2 *https://netzpolitik.org/2019/rezo-vs-cdu-wer-ist-hier-alternativlos/*
3 *https://www.youtube.com/watch?v=Xpg84NjCr9c*
4 *https://netzpolitik.org/2019/chance-verpasst-dieses-urheberrecht-bleibt-in-der-vergangenheit-stecken/*
5 *https://twitter.com/s_phre/status/1132696595445800960*
6 *http://newthinking.de/*
7 *http://re-publica.de/*
8 *https://www.facebook.com/beckedahl*
9 *http://www.amazon.de/gp/registry/wishlist/279FWSUX7VB9*

Ingo Dachwitz

Ein Jahr DSGVO: Zwölf Monate, zwölf Meinungen

Seit einem Jahr gilt die Datenschutzgrundverordnung. Wir haben Expertinnen und Experten aus der digitalen Zivilgesellschaft gefragt, wie sie die ersten 365 Tage bewerten und wie es mit dem europäischen Datenschutz weitergehen muss. Klar ist für alle: Da geht noch viel mehr.

Seit einem Jahr gilt die Europäische Datenschutzgrundverordnung und wir können zwei Dinge feststellen. Erstens ist das von einigen prognostizierte DSGVO-Armageddon ausgeblieben. Trotz des Kommunikationsdebakels[1] um ihren Start, trotz des Medienhypes um bizarre Auswüchse[2], und trotz tatsächlich geschlossener Blogs[3].

Allerdings ist zweitens bisher auch die große Datenschutzwende ausgeblieben. Zwar sind die Bürgereingaben bei den Aufsichtsbehörden stark gestiegen und Nichtregierungsorganisationen haben erste Verfahren gegen Datenkonzerne und -händler angestoßen. Zu grundlegenden Veränderungen an deren Geschäftsmodellen hat das bisher aber nicht geführt. Tatsächlich sind Verstöße gegen die DSGVO an der Tagesordnung – sei es bei Facebook[4] oder bei der Sparkasse[5]. Und auch im Netz haben Menschen weiterhin oft keine Wahl, als sich dem Tracking zu beugen oder selbst Gegenmaßnahmen[6] zu ergreifen.

Wie zufrieden kann die EU also mit ihrer Verordnung sein? Spätestens in einem Jahr soll eine offizielle Evaluierung vorliegen. Wirtschaft, Aufsichtsbehörden und Wissenschaft haben kein Problem, dabei Gehör zu finden. Weniger im Fokus stehen hin-

gegen die Perspektiven von Nutzer:innen und Bürger:innen. Wir haben deshalb zwölf nationale und internationale VertreterInnen der digitalen Zivilgesellschaft gefragt, worauf es jetzt nach dem ersten Jahr DSGVO ankommt. Hier sind ihre Antworten:

- Katharina Nocun (Aktivistin): „Selbst die DSGVO wird den großen Datenschutzproblemen nicht gerecht."
- Wolfie Christl (Aktivist): „Der kommerzielle Massendatenmissbrauch geht weiter."
- Thilo Weichert (Netzwerk Datenschutzexpertise): „Die Aufsichtsbehörden müssen sich endlich die großen Internetkonzerne vorknöpfen."
- Beata Hubrig (Anwältin): „Wir brauchen Öffentlichkeit für die unangenehmen Folgen von Datenschutzverstößen."
- Ailidh Callander (Privacy International): „Die DSGVO ist das Fundament, nicht die Decke."
- Kirsten Fiedler (European Digital Rights): „Wir sind noch weit davon entfernt, die Datensammlung zu durchblicken."
- Estelle Masse (Access Now): „Die Umsetzung in einigen Staaten ist ein Problem."
- Katarzyna Szymielewicz (Panoptykon Foundation): „Datenschutzbehörden, Zivilgesellschaft und Wissenschaft müssen zusammenarbeiten."
- Benjamin Bergemann (Digitale Gesellschaft): „Den Wächtern des Datenschutzes fehlen die Ressourcen"
- **Peter Schaar** (Europäische Akademie für Informationsfreiheit und Datenschutz): „Der Trend zu immer mehr staatlicher Überwachung ist ungebrochen"
- Kerstin Demuth (Digitalcourage): „Wir müssen unsere Rechte auch in Anspruch nehmen."
- Klaus Müller (Verbraucherzentrale Bundesverband): „Das Datenschutzniveau in Europa muss noch besser werden."

Katharina Nocun (Aktivistin):
„Selbst die DSGVO wird den großen Datenschutzproblemen nicht gerecht."

Ein Jahr nach dem angeblichen Weltuntergang leben wir alle noch und stellen überrascht fest: So viel hat sich in den meisten Bereichen gar nicht geändert. Ein Großteil der Vorgaben der DSGVO entsprechen dem Bundesdatenschutzgesetz. Höhere Strafen und strengere Vorgaben für informierte Einwilligungen sind zwar ein echter Schritt nach Vorne. Doch selbst die DSGVO wird den großen Datenschutzprobleme unserer Zeit eigentlich nicht gerecht. Hier bräuchte es flankierend starke Regeln für die ePrivacy.

Spätestens seit Cambridge Analytica muss zudem klar sein: Wir brauchen Rote Linien dafür, wie weit personalisierte Werbung gehen darf. Und in welchen Bereichen sie grundsätzlich tabu sein sollte. Denn die Grenze zwischen personalisierter Werbung und psychologischem Profiling ist längst fließend. Nach einem Jahr DSGVO können wir festhalten: Es lohnt sich, beim Datenschutz mutiger zu sein und mehr zu einzufordern.

Katharina Nocun[7] ist Publizistin und eine der bekanntesten Datenschutzaktivistinnen des Landes. Unter anderem verantworte sie bei Campact die Asyl-für-Snowden-Kampagne und war Beschwerdeführerin vor dem Bundesverfassungsgericht gegen die Bestandsdatenauskunft.

Wolfie Christl (Aktivist):
„Der kommerzielle Massendatenmissbrauch geht weiter."

Die DSGVO ist ein Kompromiss nach jahrelangen Lobby-Kriegen. Es war immer klar, dass sie weder den Überwachungskapitalismus abschaffen noch die extreme Macht der Plattformen brechen wird. Aber sie geht nicht mehr weg, und sie ist ein Fortschritt, weil sie zum ersten Mal Regeln eingeführt hat, die potenziell auch wirklich durchgesetzt werden können. Das war lange überfällig, denn Einzelne haben heute keinerlei Chance mehr, die permanente Datenauswertung zu verstehen oder ihr gar zu entkommen. Der Start war schlecht, wegen unzureichender nationaler Anpassungsgesetze und weil viel zu wenig Mittel für Information, praktische Auslegung und Hilfestellung für kleinere Datenverarbeiter zur Verfügung gestellt wurden.

Nach einem Jahr herrscht nach wie vor Verunsicherung auf der Alltagsebene. Leider ist es bisher auch nur ungenügend gelungen, das Wild-West des kommerziellen Massendatenmissbrauchs in den Griff zu bekommen. Websites und Apps übertragen nach wie vor Daten an unzählige Drittparteien. Ich habe Verständnis dafür, dass heikle Fälle mit weitreichenden Folgen für zukünftige Auslegung Zeit benötigen. Aber es braucht nun dringend Präzedenzfälle mit massiven Sanktionen, von Online-Marketing bis zu den großen Plattformen. Dafür benötigen die Aufsichtsbehörden viel mehr Mittel, und sie müssen endlich Risiken eingehen.

Wolfie Christl[8] ist Privacy-Forscher und Aktivist. Er hat sich der Aufklärung über die Strukturen des Überwachungskapitalismus verschrieben und prägt mit seinen Studien auch die internationale Debatte.

Thilo Weichert (Netzwerk Datenschutzexpertise):
„Die Aufsichtsbehörden müssen sich endlich die großen Internetkonzerne vorknöpfen."

Die Hausaufgaben, die die DSGVO uns stellt, sind weder in Europa noch in Deutschland abgearbeitet: In Europa fehlen noch die ePrivacy-Verordnung sowie viele spezifische Datenschutzregelungen, bei denen sich die Nationalstaaten überfordert zeigen, etwa zur Verarbeitung von Gesundheitsdaten oder zur Forschungsprivilegierung. Die Aufsichtsbehörden müssen sich endlich die großen Internetkonzerne vorknöpfen.

In Deutschland müssen diese Aufsichtsbehörden erst einmal angemessen ausgestattet werden, wozu mindestens eine Verdoppelung des Personals gehört. Damit ließe sich endlich auch eine sinnvolle Zertifizierung realisieren. Gesetzgeberisch liegt vieles im Argen, etwa die teils verfassungs- und europarechtswidrige Füllung der Öffnungsklauseln oder das Fehlen eines Beschäftigtendatenschutzgesetzes.

Thilo Weichert war bis 2014 Datenschutzbeauftragter vom Schleswig-Holstein. Seitdem bringt er sich im Rahmen des Netzwerks Datenschutzexpertise mit Gutachten und konkreten Vorschlägen in die Debatte ein.

Beata Hubrig (Anwältin):
„Wir brauchen Öffentlichkeit für die unangenehmen Folgen von Datenschutzverstößen."

Nachdem das Probejahr vorbei ist, sollten wir ein neues Kapitel aufschlagen und den abstrakten Regelungen mehr Leben einhauchen. Dabei denke ich besonders an das allgemein Überwachungsverbot und die strenge Zweckbindung bei der Datenverarbeitung. Wir sollten vermehrt Geschichten an die Öffentlichkeit bringen, aus denen die unangenehmen Folgen für Bürger erkennbar sind, wenn gegen diese Regelungen verstoßen werden.

Dabei liegen mir zwei Bereiche besonders am Herzen: 1. Wie werden wir wirtschaftlich manipuliert, nachdem unsere personenbezogenen Daten von Privatunternehmen ausgewertet wurden? 2. Wann werden die Akten der unzähligen Überwachungen des Verfassungsschutzes der Bundesrepublik zugänglich gemacht? Muss ein Staat, der sich Rechtsstaat nennt, erst untergehen, damit eine „Gauck-Behörde" eingerichtet wird?

Beate Hubrig[9] ist Rechtsanwältin mit den Schwerpunkten Urheberrecht und Datenschutz. Neben ihrer beruflichen Tätigkeit klärt sie in Vorträgen über die DSGVO auf und entwickelte gemeinsam mit dem Chaos Computer Club einen Generator zur Beantwortung unberechtigter Urheberrechtsabmahnungen[10].

Ailidh Callander (Privacy International):
„Die DSGVO ist das Fundament, nicht die Decke."

Was wir jetzt brauchen, ist zum einen die proaktive Umsetzung der DSGVO durch Unternehmen. Sie müssen beispielsweise die Anforderungen von „Datenschutz by design" und „by default" umsetzen. Gleichzeitig sehen wir, wie viele Unternehmen an vorderster Front dagegen kämpfen, dass die Reformen zum Schutz unserer Daten im digitalen Zeitalter abgeschlossen werden. Ein klares Beispiel ist die ePrivacy-Verordnung[11]. Doch auch die Regierungen müssen sich beweisen. Von der vollständigen Umsetzung der DSGVO und der Strafverfolgungsrichtlinie bis hin zur Schließung von Schlupflöchern, etwa Ausnahmen für politische Parteien[12]. Entscheidend ist, dass sie der Zivilgesellschaft die Möglichkeit geben, Sammelklagen einzureichen. Ohne diese ist eine wirksame Umsetzung der DSGVO kaum möglich.

Auch wenn Untersuchungen und Verfahren eine Weile brauchen, ist es nach einem Jahr an der Zeit, dass die Aufsichtsbehörden ihre ausgebauten Befugnisse nutzen und Maßnahmen zur Durchsetzung ergreifen. Erste Schritte haben wir bereits erlebt, gerichtliche Klärungen werden folgen. Mit Datenschutzgesetzen und Reformen auf der Agenda vieler Länder außerhalb der EU gibt es Anstrengungen, das Datenschutzrecht auch weltweit zu stärken. Diese Gesetze müssen so stark wie möglich sein. Für alles weitere sollten wir die DSGVO nicht als die Decke, sondern als das Fundament verstehen. [Übersetzung netzpolitik.org]

Ailidh Callander ist Legal Officer bei Privacy International[13] und dort für den Bereich Datenschutzregulierung zuständig. Die Nichtregierungsorganisation mit Sitz in London hat nach dem 25. Mai 2018 mehrere Verfahren gegen Datenhändler und Werbefirmen[14] angestoßen.

Kirsten Fiedler (European Digital Rights):
„Wir sind noch weit davon entfernt, die Datensammlung zu durchblicken."

Mit der DSGVO haben wir 2016 Regeln bekommen, die die Rechte von NutzerInnen stärken und auf alle Arten von Technologien angewendet werden können, sobald unsere Daten verarbeitet werden und solange wir als NutzerInnen in der EU ansässig sind. Leider sind wir aber noch weit davon entfernt, das Ausmaß der Datensammlung und -auswertung zu durchblicken. Intransparente Geschäftspraktiken führen weiterhin dazu, dass das Verhalten von Nutzer:innen ständig beobachtet wird und in umfassenden Profilen unglaubliche Mengen sensibler Daten zusammengeführt werden.

Seit der DSGVO dürfen Algorithmen allerdings nicht mehr allein darüber entscheiden, ob wir zum Beispiel keinen Kredit, keinen Job oder ein bestimmtes Produkt nicht angezeigt bekommen. Außerdem können wir seit der DSGVO nun verlangen, die Logik, die Tragweite und die angestrebten Auswirkungen einer automatisierten Entscheidung zu erfahren. Die Mitglieder von European Digital Rights kämpfen daher in den Europas Mitgliedstaaten mit Beschwerden bei den Aufsichtsbehörden gegen Geschäftsmodelle an, die weiterhin auf verstecktem Tracking und voraussagendem Profiling basieren. Leider fehlen den Behörden derzeit jedoch die ausreichende Finanzierung und spezialisier-

tes Personal, um die Regelungen effizient zu überwachen und durchzusetzen – das muss sich ändern!

Kirsten Fiedler[15] war lange Zeit Geschäftsführerin von European Digital Rights[16]. Die NGO mit Sitz in Brüssel ist ein Zusammenschluss digitaler Bürgerrechtsorganisationen aus ganz Europa.

Estelle Masse (Access Now):
„Die Umsetzung in einigen Staaten ist ein Problem."

Im ersten Jahr der Umsetzung der Datenschutzgrundverordnung ist die Bilanz durchwachsen. Wir haben die ersten positiven Auswirkungen der DSGVO gesehen: Menschen, die in der EU leben, haben von ihren Rechten Gebrauch gemacht, eine große Zahl von Beschwerden bei den Behörden eingereicht und die Datenschutzbehörden haben langsam begonnen, das Gesetz umzusetzen, indem erste Geldbußen verhängt wurden. Aber wir haben auch große Probleme bei der Umsetzung gesehen.

Mehrere Mitgliedstaaten haben die im Rahmen der DSGVO verfügbaren Flexibilitäten und Ausnahmen sehr breit ausgelegt, die nun zu einer Zersplitterung des Schutzniveaus für die betroffenen Personen in der gesamten EU führen könnten. Im schlimmsten Fall haben einige wenige Mitgliedstaaten nationale Maßnahmen ergriffen, die im Widerspruch zu Geist, Ziel und Text der DSGVO stehen. Die DSGVO wird nur so stark sein wie ihr schwächstes Glied. Um zu vermeiden, dass die Vorteile des Gesetzes für die Nutzer:innen beeinträchtigt werden, muss sich die EU-Kommission nun frühzeitig aller Umsetzungsprobleme annehmen.

Für die meisten war 2018 das Jahr des Erwachens des Datenschutzes in Europa. Damit die DSGVO ihr Potenzial voll ausschöpfen kann, muss 2019 das Jahr der Umsetzung sein. Ein Großteil dieser Verantwortung liegt bei den Datenschutzbehörden, die schnell und koordiniert handeln müssen. Das bedeutet, dass die Mitgliedstaaten für diese Behörden angemessene Mittel und Personalausstattung bereitstellen müssen, damit sie ihre Aufgaben effektiv erfüllen können. [Übersetzung netzpolitik.org]

Estelle Masse[17] ist Senior Policy Analyst and Global Data Protection Lead bei Access Now[18]. Die NGO setzt sich weltweit für Menschenrechte und ein offenes und freies Internet ein.

Katarzyna Szymielewicz (Panoptykon Foundation):
„Datenschutzbehörden, Zivilgesellschaft und Wissenschaft müssen zusammenarbeiten."

Die DSGVO lässt keinen Zweifel daran, dass wir als Einzelpersonen das Recht haben, personenbezogene Daten zu kontrollieren, die durch Algorithmen und statistische Analysen erzeugt wurden. Wir können auch eine Erklärung der Logik hinter der Verwendung von Algorithmen verlangen, wenn sie zu Entscheidungen mit erheblichen Auswirkungen führen. Das sind solide Prinzipien und gute Ausgangspunkte für strategische Rechtsverfahren. Wir müssen jedoch ehrlich zugeben, dass wir ein Jahr nach Inkrafttreten der DSGVO noch lange nicht in der Lage sind, diese Black Boxes zu öffnen.

Mit der Panoptykon Foundation haben wir erste Beschwerden eingereicht[19], die solche Werbemodelle, die auf konstantem, verstecktem Tracking und voraussagendem Profiling basieren, infrage stellen. Bei unseren Untersuchungen dieser komplexen Daten-Ökosysteme mussten wir feststellen, dass es Barrieren gibt, die nur starke Behörden überwinden können. Ohne Zugriff auf Server, Datenbanken und Code können wir zwar raten, aber keine zuverlässigen Beweise vorlegen. Hier müssen Datenschutzbehörden, Zivilgesellschaft und Wissenschaft über konkrete Fälle hinaus zusammenarbeiten. [Übersetzung netzpolitik.org]

Katarzyna Szymielewicz ist Mitgründern der polnischen digitalen Bürgerrechtsorganisation Panoptykon Foundation[20]. Nach dem 25. Mai 2018 brachte die NGO Verfahren gegen die Online-Werbesysteme des International Advertising Bureau und Google ins Rollen.

Benjamin Bergemann (Digitale Gesellschaft):
„Den Wächtern des Datenschutzes fehlen die Ressourcen"

Die DSGVO ist das Beste, was wir haben, um die Macht der großen Datenverarbeiter und die daraus resultierenden Risiken für unsere Grundrechte, Rechtsstaatlichkeit und das demokratische Gemeinwesen in den Griff zu bekommen. Leider wird die Anwendung der DSGVO diesem Anspruch noch nicht gerecht. Viel zu oft ging es im Jahr 1 der DSGVO um Lappalien, die mit den wichtigen Fragen der Datenmacht wenig zu tun haben. Dieser falsche Fokus resultiert nicht nur aus einem Missverständnis über das Ziel des Datenschutzes oder gezielter Öffentlichkeitsarbeit derjenigen, die an einer Schwächung des Datenschutzes interessiert sind. Er ist vor allem ein Ressourcenproblem.

Den Wächtern des Datenschutzes fehlen die Mittel, um sich mit den wirklich relevanten Problemen wie exzessiver, zweckentfremdeter und nicht überprüfbarer Datenverarbeitung zu beschäftigen. Die Bundes- und Landesregierungen, Stiftungen und Spender müssen Geld in die Hand nehmen, damit Datenschutzaufsichtsbehörden, Verbraucherschutzverbände und NGOs die Großen an den Maßstäben der DSGVO messen können.

Benjamin Bergemann[21] ist ehrenamtlicher Vorstand des Vereins Digitale Gesellschaft[22]. Die Berliner NGO setzt sich für Grund- und Bürgerrechte in der digitalen Gesellschaft ein.

Peter Schaar (Europäische Akademie für Informationsfreiheit und Datenschutz):
„Der Trend zu immer mehr staatlicher Überwachung ist ungebrochen"

Dass mit der DSGVO der Datenschutz in den EU-Ländern vereinheitlicht wurde, bewerte ich uneingeschränkt positiv. Leider haben aber mehrere EU-Länder – allen voran Deutschland und Österreich – die von ihnen durchgesetzten DSGVO-Öffnungsklauseln überwiegend nicht im Sinne eines besseren Datenschutzes genutzt. Die Gesetzgebung folgte stattdessen primär

dem Ziel, mehr Datenverarbeitung zu ermöglichen, Betroffenenrechte einzuschränken und – das gilt insb. für Österreich – eine effektive Datenschutzaufsicht zu erschweren.

Auch der Trend zu immer mehr staatlicher Überwachung ist ungebrochen. Gleichzeitig fehlen in zentralen Bereichen klare gesetzliche Vorgaben, die den Anforderungen des europäischen Rechts entsprechen, etwa beim Schutz von Beschäftigtendaten, für Internetdienste und für den Ausgleich des Datenschutzes mit der Presse- und Meinungsfreiheit. Die Hauptverantwortung für die damit verbundenen Rechtsunsicherheiten liegt nicht bei der Europäischen Union, sondern in Berlin, Wien und in den anderen Hauptstädten der EU-Mitgliedstaaten.

Peter Schaar[23] ist Vorsitzender der Europäischen Akademie für Informationsfreiheit und Datenschutz. Bis 2015 war Bundesbeauftragter für den Datenschutz und die Informationsfreiheit. Gemeinsam mit Alexander Dix hat er jüngst eine Bilanz zur Umsetzung der DSGVO[24] veröffentlicht.

Kerstin Demuth (Digitalcourage):
„Wir müssen unsere Rechte auch in Anspruch nehmen."

Die Datenschutzgrundverordnung ist ein großer Erfolg: Einheitlicher Datenschutz in Europa und Sanktionen, die auch für Großkonzernen aus dem Silicon Valley schmerzhaft werden können. Jetzt ist es wichtig, dieses Recht auch durchzusetzen: Die Datenschutzbehörden müssen so ausgestattet sein, dass die DSGVO maximal wirkt. Entscheidend wird auch sein, dass wir selber unsere Rechte in Anspruch nehmen, zum Beispiel auf Auskunft, Löschung oder Änderung unserer Daten.

Als nächstes brauchen wir eine ePrivacy-Verordnung, die ihrem Namen gerecht wird. Die Reform wird derzeit vom EU-Rat verschleppt. Jetzt soll sie sogar als Vehikel für eine Vorratsdatenspeicherung dienen. Das wäre fatal. Die ePrivacy-Verordnung ist die beste Chance, um in der Zukunft Privatsphäre in der Kommunikation und im Internet rechtlich sicherzustellen.

Kerstin Demuth ist Campaignerin und Redakteurin bei Digitalcourage. Der Verein mit Sitz in Bielefeld setzt sich für Grundrechte und Datenschutz ein.

Klaus Müller (Verbraucherzentrale Bundesverband):
„Das Datenschutzniveau in Europa muss noch besser werden."

Die Datenschutzgrundverordnung ist ein wichtiger Schritt nach vorne und ein Gewinn für alle Verbraucherinnen und Verbraucher in der EU. Der bisher oft vernachlässigte Datenschutz wird nun als wichtiges Thema anerkannt. Obwohl die Verordnung Verbraucherrechte entscheidend gestärkt hat, werden aber bereits jetzt Schwachstellen sichtbar. Die Ausstattung der Aufsichtsbehörden weist Lücken auf. Die Regelungen zu automatisierten Entscheidungen und der Profilbildung sind nicht im Sinne der Verbraucher. Hier muss im Rahmen der Evaluation 2020 nachgebessert werden.

Das Datenschutzniveau in Europa muss aber noch besser werden. Ein Baustein dazu ist die e-Privacy-Verordnung. Telekommunikationsdiensten sollte es nur mit Einwilligung oder unter strengen Voraussetzungen erlaubt werden, Kommunikationsdaten, wie beispielsweise Chatinhalte oder Standortdaten, zu verarbeiten. Auch darf es kein Tracking von Verbrauchern ohne deren vorherige Einwilligung geben. Die Mitgliedstaaten im EU-Rat können sich jedoch seit Jahren nicht auf eine gemeinsame Position einigen. Die Bundesregierung muss sich daher stärker als bisher für eine verbraucherfreundliche e-Privacy-Verordnung einsetzen.

Klaus Müller ist Vorstand des Verbraucherzentrale Bundesverbandes[25] und Mitglied der Datenethikkommission der Bundesregierung. Der vzbv ist die politische Dachorganisation der Verbraucherzentralen.

Anmerkungen

1 *https://netzpolitik.org/2018/datenschutzgrundverunsicherung-danke-merkel/*
2 *https://www.spiegel.de/netzwelt/netzpolitik/dsgvo-mythen-aus-dem-ersten-jahr-datenschutz-grundverordnung-a-1265926.html*
3 *https://netzpolitik.org/2018/die-dsgvo-und-das-blogsterben-es-ist-kompliziert/*
4 *https://netzpolitik.org/2018/facebook-nutzt-anpassung-an-datenschutzgrundverordnung-um-gesichtserkennung-auch-in-europa-zu-starten/*
5 *https://netzpolitik.org/2019/datenschutzskandal-sparkasse-erschleicht-sich-werbeerlaubnis/*
6 *https://netzpolitik.org/2018/kleines-einmaleins-der-digitalen-selbstverteidigung/*
7 *https://twitter.com/kattascha*
8 *https://twitter.com/WolfieChristl*
9 *https://twitter.com/lolaandromeda?lang=de*
10 *https://netzpolitik.org/2016/interview-warum-ein-abmahnbeantworter-der-antwortschreiben-generiert/*
11 *https://netzpolitik.org/2018/bericht-ueber-lobbyismus-wie-die-datenindustrie-die-eu-bearbeitet/*
12 *https://www.gdprtoday.org/gdpr-loopholes-facilitate-data-exploitation-by-political-parties/*
13 *https://twitter.com/privacyint*
14 *https://netzpolitik.org/2018/kampf-den-datenhaendlern-privacy-international-legt-beschwerden-ein/*
15 *https://twitter.com/Kirst3nF*
16 *https://twitter.com/edri*
17 *https://twitter.com/EstelMP*
18 *https://twitter.com/accessnow*
19 *https://en.panoptykon.org/update-complaints-against-iab-google*
20 *https://panoptykon.org/*
21 *https://twitter.com/_bberg?lang=de*
22 *https://twitter.com/digiges*
23 *https://twitter.com/peter_schaar?lang=de*
24 *https://www.gruene-bundestag.de/fileadmin/media/gruenebundestag_de/themen_az/datenschutz/Gutachten_DSGVO.pdf*
25 *https://twitter.com/vzbv*

Lesen & Sehen

Neues für Bücherwürmer & Cineasten

Grundrechte-Report – Pressemitteilung

Grundrechte-Report 2019: Grundrechte unter Druck

23. Mai 2019 – Am Donnerstag, den 23. Mai 2019 – genau am 70. Jahrestag des Grundgesetzes – stellen in Karlsruhe neun deutsche Bürger- und Menschenrechtsorganisationen den neuen Grundrechte-Report vor. In 35 Beiträgen weisen verschiedene AutorInnen auf Beispiele für die Einschränkung von Grundrechten, von Ungleichbehandlung sowie der Überschreitung institutioneller Kompetenzen in den verschiedensten Bereichen der vergangenen zwölf Monate hin.

Den diesjährigen Grundrechte-Report stellt der Rechtsanwalt und Politiker **Dr. Gregor Gysi** vor. Er ist zugleich Autor des Einleitungsartikels zu *70 Jahre Grundgesetz*. Er resümiert: „*Das Grundgesetz braucht auch 2019 den Grundrechte-Report, der mit einer Vielzahl von Beispielen, wie in unserem Land verfassungsmäßige Grundrechte missachtet und eingeschränkt werden, mahnt, nicht nachzulassen im Einsatz für deren Schutz und Verteidigung.*“ Hinzufügend kommentiert er: „*70 Jahre Grundgesetzpraxis zeigen, dass wir die Grundrechte in ihrer Substanz nur bewahren können, wenn wir sie auch ausbauen. Wir brauchen im Grundgesetz und in Europa einklagbare soziale Grundrechte, weil heute die immer tiefere soziale Spaltung in Deutschland, Europa und weltweit für immer größere Bevölkerungsgruppen Grundrechte beschneidet, zum Teil sogar ausschließt.*“

Bellinda Bartolucci, Iris Burdinski, Marie Diekmann, Rolf Gössner, Julia Heesen, Martin Heiming, Hans-Jörg Kreowski, Britta Rabe, Rosemarie Will (Hrsg.): Grundrechte-Report 2019 – Zur Lage der Bürger- und Menschenrechte in Deutschland. Fischer Taschenbuch Verlag, Frankfurt/M., Mai 2019, ISBN 978-3-596-70434-7, 208 Seiten, Preis 12.00 Euro.

Wie jedes Jahr nehmen an der Präsentation des Grundrechte-Reports Menschen teil, deren Fälle der aktuelle Grundrechte-Report behandelt:

Vera Egenberger klagte erfolgreich gegen die Praxis der Kirchen, Arbeitsstellen für Kirchenmitglieder zu reservieren: In ihrem Klageverfahren hat der Europäische Gerichtshof (EuGH) zuletzt die Möglichkeiten kirchlicher Arbeitgeber deutlich begrenzt und damit der langjährigen Praxis des Bundesverfassungsgerichts (BVerfG) widersprochen, den Kirchen vielfach arbeitsrechtliche Diskriminierungen aus religiösen Gründen zu ermöglichen. Vera Egenberger erklärt dazu: „*Diskriminierungsschutz beim Zugang zu Beschäftigung ist ein durch die Europäische Union verbrieftes Recht. In Deutschland wiederum stellt man das Recht der Kirchen, sich selbst zu ordnen, über das Recht auf die individuelle Diskriminierungsfreiheit. Das war und bleibt weiterhin problematisch, wenn konfessionellen Arbeitgebern nicht durch die Gerichte verdeutlicht wird, wo die Grenzen des Selbstbestimmungsrechts der Kirchen verlaufen.*“

Der Rechtsanwalt **Engin Sanli** setzte sich als Anwalt für einen Mann aus Togo ein, der nach einem ersten, gescheiterten Versuch mit massivem Polizeieinsatz aus der Aufnahmeeinrichtung Ellwangen abgeschoben wurde. Daraufhin erhielt Sanli Hass-Mails und Drohbriefe und wurde von führenden PolitikerInnen gar als Teil einer „Anti-Abschiebe-Industrie“ diffamiert. Mit dieser Erfahrung ist er nicht allein, aktuell geraten Beratungsstellen und RechtsanwältInnen wegen ihres Einsatzes für einen rechtsstaatlichen Umgang mit Geflüchteten mehr und mehr unter Druck. Engin Sanli kommentiert: „*Das Grundrecht auf ein faires Verfahren gilt für alle Menschen gleich. Dies sollte von PolitikerInnen öffentlich verteidigt werden. Stimmen sie stattdessen in den Chor der Hetzenden und Menschenverachtenden ein und führen ihn gar an, stellen sie damit die Demokratie in diesem Lande in ihren Grundfesten in Frage.*“

Moderiert wird die Präsentation von **Iris Burdinski**. Sie ist im Bundesarbeitskreis kritischer Juragruppen (BAKJ) aktiv und Mitherausgeberin des Grundrechte-Reports 2019.

Inhalt des aktuellen Grundrechte-Reports

Soziale und ökologische Themen erhalten im aktuellen Grundrechte-Report einen breiten Platz: Die rechtlich verfügten Fahrverbote von Dieselfahrzeugen zur Einhaltung von Grenzwerten für den Ausstoß von Stickstoffdioxid wurden von der Landesregierung Bayern beispielsweise schlicht ignoriert. Katrin Brockmann erklärt die Rolle des Bundesamts für Verbraucherschutz und Lebensmittelsicherheit (BVL) im „Glyphosat-Skandal“. Finanzielle Interessen gehen über den Klima-Schutz, dies macht Inken Behrmann an der Diskussion um den Kohleausstieg Deutschlands deutlich. Frank Wilde beschäftigt sich mit der Verbindung von Armut und Ersatzfreiheitsstrafe: Die Anordnung von Haft bei Nichtbegleichung einer Geldstrafe für geringe Vergehen betrifft in hohem Maße Menschen am Rande des Existenzminimums.

Michèle Winkler betrachtet die Gefahren der neuen Polizeigesetze der verschiedenen Bundesländer, weiterhin nimmt der aktuelle Band die Einschränkungen der Pressefreiheit sowie die Ausweitung polizeilicher Zugriffsmöglichkeiten auf persönliche digitale Daten in den Fokus. Anlässlich des 100jährigen Jubi-

läums des Frauenwahlrechts im vergangenen Jahr weist Cara Röhner auf die geringen parlamentarischen Repräsentation von Frauen hin, und Sophie Rotino stellt die bisher unbefriedigenden rechtlichen Bemühungen um eine geschlechtergerechte Sprache auf dem Prüfstand.

Ergänzung der Redaktion: *Der Grundrechte-Report 2019 enthält auch drei Beiträge aus dem unmittelbaren FIfF-Umfeld, die unterschiedliche Aspekte der Netz- und Friedenspolitik thematisieren:* Stefan Hügel *und* Rainer Rehak *schreiben über den* „Kampf um Troja – Verwundbarkeit der vernetzten Gesellschaft durch Nutzung von Schadsoftware" *(S. 23) und über* „Künstliche Intelligenz im Wahlkampf – Zentralisierung und politische Profilbildung gefährden die Demokratie" *(S. 131).* Hans-Jörg Kreowski *behandelt* „Extralegale Tötung durch Drohnen und autonome Waffen. Kampfdrohnen für die Bundeswehr". *Dazu kommen weitere Beiträge mehrerer AutorInnen zu Themen wie Überwachung und einer Zivilklausel an Hochschulen.*

Inhaltsverzeichnis: http://www.grundrechte-report.de/2019/inhalt/

Trägerkreis: Der Grundrechte-Report 2019 wird gemeinschaftlich herausgegeben von der Humanistischen Union, dem Bundesarbeitskreis Kritischer Juragruppen, der Internationalen Liga für Menschenrechte, dem Komitee für Grundrechte und Demokratie, der Neuen Richtervereinigung, von Pro Asyl, dem Republikanischen Anwältinnen- und Anwälteverein, der Vereinigung Demokratischer Juristinnen und Juristen und dem Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung.

Dagmar Boedicker

Steffen Mau – „Das metrische Wir – Über die Quantifizierung des Sozialen"

Steffen Mau *zeigt anschaulich, was IT-Fachleute und andere im Einzelnen kritisieren und Algorithmen-Versteher im Feuilleton beklagen. Er zeichnet ein Gesamtbild davon, was unter der Wasseroberfläche liegt vom Eisberg, der uns frösteln lässt. So können das wohl nur Soziologinnen und Soziologen. Er beschreibt, wie Staat, Experten, Unternehmen und wir selbst durch verinnerlichte wie externe Quantifizierung die Gesellschaft und ihre Werte verändern. Er erklärt, wieso wir die Legitimität solcher Messungen, der abgeleiteten Anforderungen und den Wettbewerb sogar auf „Quasi-Märkten" als „natürlich und unhinterfragbar" (S. 188) hinnehmen.*

Vertrauen ist gut, Kontrolle ist besser: Die Volksrepublik China hat erklärt, mit ihrem *Social Credit System* gesellschaftliches Vertrauen herstellen zu wollen. Das Mittel der Wahl ist totale soziale Kontrolle. Wer glaubt, dass das in Europa ausgeschlossen ist, hat noch nicht genau genug hingeguckt. Auch bei uns soll durch eine Datensammelwut das „Steuerungswissen" für Eingriffe erhöht werden und die verschiedenen gesellschaftlichen Akteure machen (mehr oder weniger) begeistert mit bei dem, was technisch möglich ist. Sie stellen nicht nur ihre Daten zur Verfügung, sie akzeptieren die Bewertungen daraus und übernehmen sie für ihre individuelle Selbststeuerung. Damit geben sie ihre Freiheit auf, unabhängig von den abgeleiteten Leistungs- und Verhaltenserwartungen zu handeln.

Steffen Mau:
Das metrische Wir – Über die Quantifizierung des Sozialen.
Suhrkamp Verlag.
Klappenbroschur,
308 Seiten,
Preis 18,50 Euro.
ISBN: 978-3-518-07292-9

Ganz offensichtlich bildet die Ökonomisierung der letzten Jahrzehnte den fruchtbaren Nährboden für eine solche Steuerung durch Kennzahlen und andere quantifizierbare Kriterien. Viele Autorinnen und Autoren haben sich damit auseinandergesetzt – Maus Literaturverzeichnis hat mehr als 20 Seiten.

Benennungsmacht

Wer weist Status und Reputation im Bildungs- oder Gesundheitssystem zu, in der öffentlichen Verwaltung oder an der Börse? Wer ist das in unserer Gesellschaft?

Klassifikationen ergeben sich aus gesellschaftlichen Auseinandersetzungen: Wer Indikatoren vergeben, wer messen und beschreiben darf, darf schließlich auch beurteilen und bewerten. Darf Komplexität reduzieren und Konsequenzen empfehlen oder vorschreiben und über Wert und Unwert entscheiden, denn danach müssen sich die Akteure in einem Sektor richten, bei Strafe des Scheiterns oder der Ächtung.

> *„Jede Benennung ist der Versuch, eine spezifische Lesart sozialer Phänomene zu etablieren. Gelingt es, Verständnisweisen und die Art, wie über sie kommuniziert wird, zu prägen, kann diese Lesart eine hegemoniale Stellung beanspruchen. Benennungsmacht beeinflusst dann den Comon Sense einer Gesellschaft, also sozial geteilte und daher geltende Vorstellungen der Angemessenheit, die zudem häufig institutionell verankert werden …" (S. 187)*

Das institutionelle Gefüge bestimmt mit Laufbahn, Einkommen, Status die Lebenschancen der Akteure. Um so wichtiger ist es, von Anfang an bei den Auseinandersetzungen um die richtige Art der Messung mitzumischen. Wie es die Zertifizierungs- und Ranking-Stellen an den akademischen Einrichtungen

taten, nicht aber die Hochschulen selbst. Wie sich Ökonomie entwickelte: „Omnipotente[n] Bewertungsagenturen" machen deutlich, „dass Märkte heutzutage nicht länger in Staaten eingebettet sind, sondern Staaten in Märkte." (S. 94) Der Autor betrachtet viele Bereiche unseres Alltags, von der Arbeitswelt zu den *sozialen* Netzwerken, vom Konsum- und Kommunikationsverhalten bis zum Politischen, wo der Wettbewerb der Individuen den Kampf der Klassen abgelöst hat. Er erforscht die Macht der Zahlen, ihre Hierarchisierung und die Statusmarker, wie sie funktionieren, und was ihre Risiken und Nebenwirkungen sind. Dazu gehören der Verlust von professioneller Kontrolle oder Diversität und natürlich die Überwachung. Hier zitiert er Byung-Chul Han: „Als selbstausleuchtendes, selbstüberwachendes Subjekt führt es ein *Panoptikum* seiner selbst mit sich, indem es Insasse und Aufseher zugleich ist. [...]" (S. 251)

Fazit: Absolut lesenswert! Mau fügt die Kritik an Quantifizierung und Ökonomisierung zu einer sehr gelungenen Analyse der „Psychopolitik" zusammen (man muss dazu nicht Byung-Chul Han gelesen haben).

Wissenschaft & Frieden 2/2019 „Partizipation – Basis für den Frieden"

Die Ausgabe 2/2019 von Wissenschaft & Frieden nimmt sich mit dem Schwerpunkt „Partizipation" eines Themas an, das als wichtige Stellschraube für den Frieden angesehen werden muss. Ohne die Teilhabe des Einzelnen können der Aufbau und die Wahrung des Friedens nicht realisiert werden. Deswegen untersuchen die W&F-AutorInnen die Bedeutung von Teilhabeprozessen für den Frieden, beleuchten unterschiedliche Formen der Teilhabe und fragen, welche Dinge, Personen, Systeme und Gegebenheiten Partizipation ermöglichen oder erschweren bzw. verhindern.

Es schreiben:

- *Klaus Harnack*: Die These der partizipativen Sättigung
- *Christine Meissler*: „Shrinking Space" – Einschränkungen der Arbeit in und an Konflikten
- *Laima Eicke*, *Maja Hoffmann*, *Thomas Kopp*: Gemeinsam entscheiden – Perspektiven und Risiken von Partizipation für eine sozial-ökologische Transformation
- *María Cárdenas*: „Nicht ohne uns!" Der partizipative Friedensprozess in Kolumbien
- *Kuymi Thayari Tambaco Díaz* und *Andrea Sempértegui*: Die Minga aus den Anden – Praktiken der Partizipation zur Gemeinschaftsbildung
- *Janina Rott* und *Max Schulte*: Bewegte Forschung – Protest zwischen Wissenschaft und Politik
- *Susanne Tönsmann* und *Anne Harnack*: Citizen Science – Partizipation von BürgerInnen in Forschung und Wissenschaft
- *Ulrich Wohland*: Partizipation der Friedensbewegung – Radikal und pragmatisch

Außerhalb des Schwerpunkts geht es um die besonderen Auswirkungen von atomarer Strahlung auf Frauen (John Borrie et. al.) sowie um den Militär- und Kriegsdienst der Militärseelsorge (Albert Fuchs). W&F dokumentiert den Aufsehen erregenden Beschluss des Oberverwaltungsgerichts NRW zur Nutzung von Ramstein für Drohneneinsätze der USA im Jemen. Die von Jürgen Nieth kommentierte Presseschau gibt einen Überblick über das Echo auf den weltweiten Rüstungsrekord 2018.

Dossier: „Verifikation nuklearer Abrüstung"

Die nukleare Rüstungskontrolle und Abrüstung sind in eine schwere Krise geraten. Diese Krise zu lösen und Rüstungskontrolle zu erhalten wird schwer genug; um darüber hinaus zukünftig bedeutende Reduktionen nuklearer Arsenale zu erreichen, sind u. a. neue Verifikationsverfahren und -vereinbarungen notwendig, die geeignet sind, reale Abrüstung zuverlässig zu überprüfen. Das W&F beiliegende – und zusammen mit dem Forschungsverbund *Naturwissenschaft, Abrüstung und internationale Sicherheit* (FONAS e. V.) herausgegebene – *Dossier 88* beleuchtet das Thema aus verschiedenen Blickwinkeln.

Wissenschaft & Frieden, 2/2019: „Partizipation – Basis für den Frieden", 9,00 € Inland, EU plus 3,00 € Porto (Bitte um Vorkasse: Sparkasse KölnBonn, DE86 3705 0198 0048 0007 72, SWIFT-BIC COLSDE33XXX)

W&F erscheint vierteljährlich. Jahresabo 35 €, ermäßigt 25 €, Ausland 45 €, ermäßigt 35 €, Förderabo 60 €. W&F erscheint auch in digitaler Form – als PDF und ePub. Das Abo kostet für Bezieher der Printausgabe zusätzlich 5 € jährlich – als elektronisches Abo ohne Printausgabe 20 € jährlich.

Bezug: W&F c/o BdWi-Service, Gisselberger Str. 7,
35037 Marburg, E-Mail: *service@wissenschaft-und-frieden.de*,
www.wissenschaft-und-frieden.de

Wissenschaft und Frieden ist Trägerin des Göttinger Friedenspreises 2018

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	Rainer Rehak, Benjamin Kees, Stefan Hügel
V.i.S.d.P.	Stefan Hügel
FIfF-Überall	Beiträge aus den Regionalgruppen und den überregionalen AKs. Aktuelle Informationen bitte per E-Mail an *hubert.biskup@gmx.de*. Ansprechpartner für die jeweiligen Regionalgruppen finden Sie im Internet auf unserer Webseite *https://www.fiff.de/regionalgruppen*
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	Motiv des Tagungsplakats der FIfFKon 2018
Druck	Meiners Druck, Bremen

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.

Nachdruckgenehmigung wird nach Rücksprache mit der Redaktion in der Regel gern erteilt. Voraussetzung hierfür sind die Quellenangabe und die Zusendung von zwei Belegexemplaren. Für unverlangt eingesandte Artikel übernimmt die Redaktion keine Haftung.

Wichtiger Hinweis: Wir bitten alle Mitglieder und Abonnenten, Adressänderungen dem FIfF-Büro möglichst umgehend mitzuteilen.

Aktuelle Ankündigungen

(mehr Termine unter *www.fiff.de*)

FIfFKon19 „Künstliche Intelligenz als Wunderland"
22.–24. November in Bremen

FIfF-Kommunikation

3/2019 „IT-Security und Cyberpeace"
M. Ahlmann, S. Johnigk, H.-J. Kreowski, K. Nothdurft
Redaktionsschluss: 2. August 2019

4/2019 „Überwachungsgesamtrechnung"
Dagmar Boedicker u. a.
Redaktionsschluss: 1. November 2019

1/2020 „Künstliche Intelligenz als Wunderland"
Michael Ahlmann, Hans-Jörg Kreowski u. a.
Redaktionsschluss: 7. Februar 2020

W&F – Wissenschaft & Frieden

2/18 Wissenschaft im Dienste des Militärs?
(mit Dossier 86: Cyberrüstung und zivile IT-Sicherheit)
3/18 Gender im Visier
4/18 Kriegsführung 4.0
(mit Dossier 87: AfD, PEGIDA & Co.)
1/19 70 Jahre NATO
2/19 Partizipation – Basis für den Frieden
(mit Dossier 89: Verifikation nuklearer Abrüstung)

vorgänge – Zeitschrift für Bürgerrechte und Gesellschaftspolitik

#223 Bürgerrechte im Sport
#224 Der Osten als Vorreiter? Rechtspopulismus im Gefolge wirtschaftlicher und politischer Umbrüche
#225 Wandel der Kommunikationsfreiheit durch Digitalisierung und Internet
#226 Polizei und Technikeinsatz

DANA – Datenschutz-Nachrichten

3/18 Big Data und KI
4/18 Technischer Datenschutz
1/19 Social Media
2/19 Ein Jahr DSGVO – ein Résumé

Das FIfF-Büro

Geschäftsstelle FIfF e. V.
Ingrid Schlagheck (Geschäftsführung)
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

Schluss FIfF

Photo by arvin keynes on Unsplash

Geeignete Texte für den SchlussFIfF bitte mit Quellenangabe an *redaktion@fiff.de* senden.