The Hank Show : how a house-painting, drug running DEA informant built the machine that rules our lives / McKenzie Funk. – 1. Auflage – New York, NY : St. Martin's Press, 2023. – viii, 296 Seiten. – ISBN 978-1-250-20927-6 : USD 30.00 (auch als E-Book verfügbar)

Sich vorzustellen sei angebracht, meint der Autor zu Beginn des Buches. Sein Name sei McKenzie Funk, seine LexID 000874529875. Diese LexID sei 2001 erstellt worden und unterscheide ihn seitdem trennscharf etwa von McKenzie Funk aus dem Bundestaat Nebraska (LexID XXXXXXXX9429) oder McKenzie Funk aus Ohio (LexID XXXXXXXX2145). Soweit klingt dies auch im wissenschaftlichen Informationswesen vertraut, wo man von ORCIDs, normierten Personennamen und anderen Identifiern umgeben ist. Die LexID 000874529875 verknüpft aber nicht (nur) diese eine Person mit Texten, sondern sammelt Datenpunkte in ganz anderem Umfang: die Geburtsurkunde, Angaben zu den Eltern, den Angelschein des Jugendlichen, den Führerschein, das besuchte College, den ersten Arbeitgeber. Damit sind schon genug Angaben zusammen, um zu erkennen, dass dieser McKenzie Funk offenbar weiß ist und einen relativ privilegierten Hintergrund hat. Hiermit endet der Zustrom aber noch lange nicht:

„When I opened my first credit card, it got that; when I rented an appartment in New York City, it got that; when I bought a cheap car and drove across the country, it got that; when I signed up for a travel-booking site using my email adress, it got that; whenever I shipped a package via UPS, it got that; whenever I donated to a political candidate, it got that; and when I secured a mortgage and bought my first house in Seattle, it got that." (S. 3f.)

Die LexID macht die Lebensumstände dieses Menschen sichtbar, seinen Biorhythmus, die Vorlieben, die Hobbies und das Netzwerk an Menschen, die teils ephemer, teils intensiv das soziale Umfeld bilden. Sie beeinflusst damit die ärztliche Versorgung, aber auch, wie teuer die Autoversicherung ist, welche Kreditkarte zur Verfügung gestellt wird und wie lange McKenzie Funk in der Hotline warten muss. Die LexID und ihre konkurrierenden Identifier ermöglichen somit, was Shoshana Zuboff *prediction products* nennt, nämlich die maschinelle Auswertung und Analyse von menschlichem Verhalten durch Polizei, Banken, Nachrichtendiensten, Versicherungen, politischen Parteien und die Marketingindustrie, um das Verhalten vorhersagen und ausbeuten zu können. Identifier wie die LexID oder eben die Voter_id von Cambridge Analytica stützten in den USA die Last Minute-Kampagnen in den Swing States, die ihrerseits möglicherweise Trump die Präsidentschaft sicherten. In der Pandemie ermöglichten sie das *contact tracing*, bei den Protesten gegen die Ermordung von George Floyd sollen sie die Gesichtserkennung der Menschen in der Menge unterstützt haben, während die über ihnen kreisenden Überwachungsdrohnen die IMSI-Nummern, also die Mobilnetzkennungen, aus den Handys der Protestierenden saugten.

Diese Identifier bauen einen *shadow knowledge graph* zu jeder Person auf, die sie erfassen. Sie sind Teil einer Entwicklung, die im Vergleich zu »früher« sehr ungewöhnlich ist, nämlich einer zuvor so nicht möglichen Aufspaltung von Kennen und Wissen. Auch wenn Herrschaftstechnologien schon

immer professionell neugierig waren, wusste man im gesellschaftlichen Alltag im Wesentlichen dann etwas über jemanden, wenn man ihn kannte. Im Kontakt entspann sich ein Netz an Informationen über die Person und bildete sich ein Verständnis dafür, wie sie »tickt«. Jetzt kann man so viel über jemanden wissen, dass man sein typisches Verhalten vorhersagen kann, ohne ihn in irgendeiner Weise persönlich zu kennen oder ihn jemals getroffen zu haben. Die Technologie dafür heißt *data fusion* und Identifier wie die LexID sind ihre tragenden Elemente. Der Grund, aus dem McKenzie Funk sich dafür interessiert, ist deshalb nicht der Datenschutz, wie man meinen könnte, sondern es geht ihm um die Macht, die diese Technologien ermöglichen. Wenn jede*r eine LexID hat, weiß diese auch von jeder und jedem, ob eine Rechnung noch nicht bezahlt ist, ob der Bruder mal im Knast war, ob man selbst in der Psychiatrie war oder eine Therapie brauchte, ob man mal an der Obdachlosigkeit vorbeischrammte usw. – Der Identifier zählt, rechnet auf, bewertet und greift damit in die Grundlagen der freien demokratischen Entfaltung und der sozialen Mobilität ein:

„A world in which computers accurately collect and remember and thereby make decisions based on every little thing you've ever done is a world in which your past is ever more dominant of your future. It's a world tailored to who you've been and not who you plan to be, one that perpetuates the lopsided structures we have, not those we want. It's a world in which lenders and insurers charge you more if you're poor or Black and less if you're rich or white, and one in which advertisers and political campaigners know exactly how to press your buttons by serving ads meant just for you. It's a more perfect feedback loop, a lifelong echo chamber, a life-size version of the Facebook News Feed, and insofar as it cripples social mobility because you're stuck in your own pattern, it could further hasten the end of the American Dream." (S. 10f.)

Wie ist diese Welt entstanden? Sie ist verbunden mit einem Namen, den außer Spezialisten wahrscheinlich kaum jemand kennt: Hank Asher, der von seinem Umfeld entweder gehasst oder verehrt wurde, dessen Jähzorn für fausttiefe Löcher in seinen Bürowänden sorgte und dessen gesamter *Larger-Than-Life*-Charakter für die Wendung sorgte, die den Buchtitel bildet – „The Hank Show". Asher, im Bundesstaat Indiana der Nachkriegsjahre in bürgerlichen Verhältnissen, aber mit einem ihn misshandelnden Vater aufgewachsen, verließ mit 16 die Schule und begann in einem Malereibetrieb zu arbeiten. Er zog um nach Florida, um die Winterpause zu umgehen, und machte dort seinen eigenen Betrieb auf, der rasch auf hundert Mitarbeiter wuchs. Dann entdeckte er etwas noch Lukrativeres und stieg 1982 in den Kokainschmuggel ein, um als Pilot zwischen Florida und den Bahamas zu pendeln. Als die Sache so langsam heiß wurde, wechselte er die Seiten und arbeitete als Informant für die Drug Enforcement Administration (DEA), die zentrale Drogenbehörde der USA.

Dort kam Asher in Kontakt zu dem Arbeitsgebiet, auf dem sich bald sein übergroßes Naturtalent zeigte: die DEA war die erste Law Enforcement Agency, die mit einer zentralen Datenbank arbeitete. Verdächtige wurden im System erfasst, bekamen einen Identifier und blieben dort für immer gespeichert, egal ob sie je gefasst oder verurteilt wurden oder als unbedeutend wieder aus dem Blick gerieten. Der Informant Asher fütterte seine Informationen in die Maschine, bis er sich eines Tages selbst einen Computer kaufte und begann, programmieren zu lernen. Seine neue Firma Database Technologies nahm wieder einen raschen Aufschwung, weil Asher etwas Ungewöhnliches zu eigen war: Was heute Algorithmen erkennen, nämlich Muster, sah er selbst sogar noch im trübsten Gewirr

an Informationssplittern auf seinen immer größeren Monitoren. Mehr Informationen bedeuteten dabei mehr Muster und das erzwang immer wieder technische Aufrüstungen. Asher wurde einer der frühen Anwender von *parallel computing* und ebenso einer der ersten, der eine *in memory database* aufbaute. Abfragen, für die seine Konkurrenten tagelang brauchten, konnte er in wenigen Minuten liefern.

Aber woher kamen all diese Informationen? Wir reden heute viel von Datenschutz, aber der Privacy Act in den USA stammt bereits von 1974. Wir reden viel von Informationsfreiheit und Transparenzgesetzen, aber die Transparenzgesetzgebung geht in Florida bis ins Jahr 1909 zurück. Was hatte Asher also gemacht? Er hatte gesehen, dass all diese Regelungen Abwehrrechte gegenüber dem Staat waren. Denn der Staat sollte keine Geheimnisse gegenüber den Bürgern, aber die sollten sie gegenüber dem Staat haben können. Asher war nun nicht der Staat, also besorgte er sich eine Anwältin und begann, die Daten aus den öffentlichen Stellen herauszuholen. 1993 kosteten ihn alle 14,5 Mio. Führerscheindaten Floridas $7.000, womit er seine Kunden, die Versicherungen, bediente. Aber sowohl die wie seine anderen Kunden wollten mehr, und so rauschten immer weitere Datentypen in seine Server: Fahrzeughalter, Firmenverzeichnisse, Standesamtsdaten wie Eheschließungen und Scheidungen, Schwerbehinderungen, Immobilieneigentum, Konzessionen – bereits ein Jahr später hostete seine Firma *Database Technologies* zwei Terabyte Daten. Zukäufe von anderen Firmen kamen hinzu und erbrachten Daten über Insolvenzen, Telefonverzeichnisse, Adressänderungen. 1997 öffnete sich schließlich die Büchse der Pandora: Kreditkartendaten, Sozialversicherungsnummern und die Daten der Versorgungsunternehmen. Damit konnte man Ashers Produkt *AutoTrack* nicht mehr entkommen.

„Most of what AutoTrack knew had little to do with the nascent internet. It had little to do with how careful you were. It had little to do with consent. AutoTrack knew what it knew not because you logged in to a website or filled out a warranty card and failed to read the fine print. AutoTrack knew you because in the universe of hard data Asher dealt in, there was rarely a mechanism to opt out. It was inescapable." (S. 71)

Diese Maschinerie beendete somit alle potentiellen Geheimnisse der Bürgerinnen und Bürger und begründete stattdessen das, was heute als *Risk Solutions*, *Risk Analysis* oder *Identity Solutions* umläuft, wobei alles eine bestimmte Perspektive verfolgt, nämlich die eines grundsätzlichen Misstrauens. Teils liegt das in der Natur der Kunden, denn Banken und Versicherungen leben davon, Risiken zu managen und Kreditausfälle oder Deckungsrisiken zu kalkulieren. Teils liegt es aber an etwas, das McKenzie Funk den *paranoid style in american computing* nennt. Die *Risk Industry*, die Asher begründete, unterscheide sich in ihrem Blick auf die Welt grundsätzlich etwa vom Marketing. Kümmere sich dieses um Shampoo und Automarken und stelle Fragen danach, was einem potentiellen Kunden wohl gefallen und was er vielleicht als Nächstes kaufen könnte, so stelle *Risk* Fragen wie: Was verbirgt diese Person vor uns? Was wird sie als nächstes Schlimmes tun? Und Asher, der den Schatten seiner Drogenkriminalität zeitlebens versteckte und misstrauisch bewachte, erwies sich als der perfekte Kandidat dafür, der *Risk Industry* ihre Werkzeuge zu bauen. „It was as if Asher […] had started encoding a certain paranoia – his own – into American life." (S. 63)

Daher war es nur konsequent und absehbar, dass AutoTrack und die Folgesysteme in den entsprechenden politischen Konstellationen ihre Datenauswertungen an den Staat zurückspielten, von dem

sie einen Großteil der Daten bezogen hatten. Database Technologies polierte Floridas Wählerverzeichnis so lange, bis Bush die Wahl gegen Gore gewinnen konnte (vgl. S. 94ff.) und der Topos vom angeblichen *voter fraud* geboren war, der seitdem in den Kanon der einschlägigen Akteure fest aufgenommen wurde, um das Gerrymandering – das politisch motivierte Zuschneiden von Wahlkreisen – auch virtuell immer weiter treiben zu können. Entscheidend wurde aber die Zusammenarbeit mit der Polizei, die mit einem Besuch von Leigh McMorrow, einer Mitarbeiterin vom nahe gelegenen Boca Raton Police Department, begann. Asher habe sie kaum angesehen, berichtet sie, an seinem Rechner herumgetippt und sie alle möglichen Daten über sich bestätigen lassen. Bis sie aufstand und um den Schreibtisch herumging, um zu sehen, was er sah:

„‚How are you doing that?' she wondered aloud. He explained that he was gathering public records to build a product for the insurance industry. ‚I was just so flabbergasted', McMorrow says. ‚The minute he showed it to me, I'm like, my God, oh my God. I said »You're sitting on a gold mine. Law enforcement will eat this up with a spoon.«'". (S. 73)

Und so kam es dann auch. McMorrow heuerte bei Asher an und überall, bei jeder Vorführung, war die Reaktion die gleiche: „They freaked out over it, absolutely freaked out over it" (S. 73) – und die Subskriptionen regneten. Der Staat, der keine Geheimnisse haben durfte, konnte sich die aneignen, die seinen Bürgerinnen und Bürgern genommen worden waren (oder ihnen zugerechnet wurden). Asher lehrte seine Maschine, wie ein Polizeihirn zu denken und entsprechende Suchen anbieten zu können. Hat ein Polizist die Adresse eines Verdächtigen, was will er dann wissen? Wer die Nachbarn sind. Was noch? Alle Telefonnummern, um sie abtelefonieren zu können. Suchfunktion um Suchfunktion kam hinzu: geographische Einschränkungen nach Postleitzahlen, Größe des Menschen, Geschlecht, Ethnie, Farbe des Autos – es war ein Fest.

Asher war nicht allein auf dem Datenmarkt. So wie er seine Tätigkeit an der Ostküste, von Florida ausgehend, von Bundesstaat zu Bundesstaat ausdehnte, gingen andere von der Westküste aus vor. Ein Konkurrent Ashers dürfte den Bibliotheken allgemein bekannt sein: Reed Elsevier. Während deren erster Anlauf, bei LexisNexis Data Brokering-Funktionen direkt zu installieren, zum Fiasko geriet und um ein Haar eine staatliche Regulierung der ganzen Branche provoziert hätte, gelang der zweite Anlauf umso besser, als man Ashers zweite Firma Seisint mit dem Produkt Accurint aufkaufte.

Asher hatte noch am 11. September 2001 die Türen weit aufgemacht für alles, was sich nach den Terroranschlägen unter dem Dach des 2002 gegründeten *Department of Homeland Security* sammeln sollte. Er hatte dessen Mitarbeitern den Zugang kostenlos angeboten und mit eigenem Geld extra geschützte Rechnerräume bauen lassen für die vielen diskreten Gestalten aus den diversen Diensten, die dort hineinströmten. Er passte seine Algorithmen an und fischte binnen kurzer Zeit *persons of interest* aus seinem Datenfundus heraus. Und damit konnte der *War on Terror* an „Big Brother's little helper", wie Aktivisten Asher und seinesgleichen nannten (S. 120), outgesourct werden. Ab da spannten sie das *American Dragnet* auf, dem keine Person mehr entrinnen sollte.[1] Aber Hank Asher

1 Vgl. Georgetown Law Center on Privacy & Technology: American Dragnet. Data-driven Deportation in the 21st Century, https://americandragnet.org/, Stand: 20.02.2024.

brannte zusehends aus. Er musste sich in Behandlung begeben und Seisint stand zum Verkauf – eine Gelegenheit, die Reed Elsevier nutzen wollte, obwohl sie in den Verkaufsgesprächen zunächst nicht im Vordergrund standen:

„‚Everybody considered it a stodgy old British company that couldn't move fast enough to make something like that happen,' says Andy Perlmutter […] who spent weeks holed up in the Embassy Suites as a consultant to Reed Elsevier. But for Reed Elsevier, whose leadership had their eyes opened to new opportunities by 9/11 just as their bread and butter – publishing – was being hit by the explosive growth of the World Wide Web, the fight felt existential. The company's business was more than three-quarters print, making it ‚a possible early contender to be entirely disintermediated by the internet,' as in-house venture capitalist Tony Askew put it to an interviewer years later. It had to quickly transition to something more durable, so it did." (S. 137)

LexisNexis hatte schon früher begonnen, Daten zu sammeln, da die Kernkundschaft hier ebenfalls immer mehr Fragen über Personen stellte. Der Scheidungsanwalt wollte wissen, wie es mit der Yacht des Ehemannes aussah, der Strafverteidiger suchte einen fehlenden Zeugen. Daher griff Reed Elsevier im Juli 2004 zu und kaufte Seisint für $775 Millionen in bar. Es war der zweite wesentliche Wachstumsschritt der Firma, nachdem Elsevier 1991 Pergamon Press von Robert Maxwell, einer vergleichbar rüden Gründergestalt, für £440 Millionen erworben hatte.[2] Reed Elseviers Kunden standen nun Antworten auf alle personenbezogenen Fragen offen und aus dem früheren Accurint Data Link wurde die LexID.

Selbstverständlich war es in der Folge mit der oft generösen Preisgestaltung aus Ashers Zeit vorbei. LexisNexis setzte die Preise herauf, so wie Elsevier es nach dem Kauf von Pergamon getan hatte. Weitere Kontakte und Investments kamen hinzu, so bei Ashers *brother in paranoia* Peter Thiel, bei dessen Firma *Palantir* Reed Elsevier neben der CIA der erste maßgebliche Inverstor war. Weitere Investments in strategische Kompetenzen wie Gesichtserkennung und Verhaltensbiometrie dauern bis heute an.

Hank Asher starb 2012, bevor seine letzte Firma, die er nach Ablauf der Kaufvertragsklauseln an den Start bringen wollte, Fuß gefasst hatte. Sein Erbe lebt jedoch intensiver weiter als je zuvor – wie seine Firma Accurint in LexisNexis Risk Solutions aufging, so die erste Firma AutoTrack in Thomson Reuters Konkurrenzprodukt CLEAR. Die Datenbestände wachsen, ebenso die Anwendungsgebiete, wenn z.B. *facial recognition* als digitales Instrument zur Überwachung der Offline-Welt eine neue Unentrinnbarkeit erzeugt: „You could delete your social media account. You could leave your phone at home. You couldn't leave your face at home." (S. 197) Wem das nach chinesischen Zuständen riecht, der liegt gar nicht so falsch. Denn was für die einen der *social credit score* ist, sind nach McKenzie Funk für die anderen die *alternative data*: „We feel like all data is credit data", lässt der Gründer der 2009 gegründeten Firma Zest.ai verlauten. (S. 206) Bonitätsscores wie von FICO, am ehesten noch der Schufa in Deutschland vergleichbar, genügten nicht mehr. Zest.ai, von Peter Thiel als Investor gestützt, schickt

2 Vgl. Buranyi, Stephen: Is the staggeringly profitable business of scientific publishing bad for science? The Guardian, 27.01.2017, https://www.theguardian.com/science/2017/jun/27/profitable-business-scientific-publishing-bad-for-science, Stand: 20.02.2024.

tausende Datenpunkte durch seine machine learning-Modelle, darunter die Web-browsing history, das Einkommen der Freunde, Schreibfehler beim Kreditantrag und vor allem – Daten von LexisNexis.

„As the Obama era ended and the 2016 presidential election approached, America was already awash in consumer scores. There were renter scores, juror scores, voter scores, customer-lifetime-value scores, welfare-benefits scores, and now socioeconomic health scores, many of them built upon profiles first drawn by Asher. We were constantly stalked by secret identifiers. We were constantly stalked by secret scores. It was just that, unlike our counterparts in China, whose dystopia we mourned, most of us didn't know it." (S. 208)

Wir wissen, wie es weiterging: Cambridge Analytica als das „Palantir of Propaganda" (S. 203) tat das seine, um Trump über die Ziellinie ins Präsidentenamt zu helfen, und benutzte dazu nicht nur Daten von Facebook, wo die Nutzer*innen Data Fusion sozusagen in unbezahlter Heimarbeit erledigen, sondern auch klassische Data Broker wie Axicom, um über die vergebene Voter_id dann alle erlangten Profile zu scoren. LexisNexis und Thomson Reuters schlossen große Verträge mit der berüchtigten Bundesbehörde *Immigration and Customs Enforcement* (ICE), die auf Basis der Daten ihre Razzien vornimmt, um Einwanderer zu deportieren. Die Pandemie gab *paranoid computing* die Gelegenheit, endgültig den Public-Health-Bereich zu beherrschen und, mehr noch, Triage-Entscheidungen mit Daten zu unterfüttern. Wer an das Beatmungsgerät darf? Hängt halt vom Score ab. (Vgl. S. 226 ff.)

Die Geschichte der Data Fusion zeigt in der Summe, dass sie für die politische, wirtschaftliche und soziale Machtausübung unwiderstehlich ist und außerdem dabei hilft, die von Sarah Lamdan analysierten Datenkartelle zu etablieren.[3] Lamdan wie Funk zeigen dabei gleichermaßen, dass dieser ungebrochene Erfolg eigentlich erstaunlich ist, denn geht man bei der Beurteilung selbst einfach nach Datenlage vor, dann ist die Entwicklung - auch ohne den Blick auf den enormen Flurschaden für die freiheitliche Demokratie - als mindestens durchwachsen anzusehen. Reports des U.S. Senats über die *fusion centers* fanden zwar Hinweise auf Heerscharen von Datenschutzverstößen, „but – despite an estimated billion dollars in taxpayer support – no evidence they had helped stop any terror attacks." (S. 184) Fälschliche Evidenz befördert dagegen die Falschen ins Gefängnis wie jenen John Newsome, dessen Geschichte McKenzie Funk erzählt. Die schlampige Bedienung von LexisNexis brachte ihn um seine mühsam aufgebaute Existenz und zeitweilig um sein Vertrauen in die Welt. Er hielt durch, ohne ein Schuldgeständnis zu unterschreiben. Seine Familie schaffte es, einen Anwalt zu bezahlen – und daher sieht er sich als einen Glückspilz an, denn „there's plenty of people that could tell you the story that I'm telling you right now. But they're gonna tell it to you, and the ending of theirs is gonna be like, ‚and when I got out of jail fifteen years later…'" (S. 189) Data Fusion schafft eben Masse und umgehend erledigte Fälle, so wie die Grenzpolizei ICE auch die einfach zu Findenden greift: Mütter, die vor ihren kleinen Kindern verhaftet werden oder steuerzahlende Arbeitnehmer in ihrem Betrieb. Die Verhaftungen füllen die Quote an Abschiebungen, mit denen politische Stärke demonstriert werden kann. (Vgl. S. 212ff.)

3 Vgl. Lamdan, Sarah: Data Cartels. The companies that control and monopolize our information, Stanford 2023 sowie die Rezension hier in: o-bib. Das offene Bibliotheksjournal 9(4), 2022, S. 1-8. Online: https://doi.org/10.5282/o-bib/5902.

Data Fusion ist heute ein Multimilliardenmarkt, der nach Marktprognosen mit 15-20 % jährlich wächst.[4] Marktbestimmend ist eine äußerst überschaubare Anzahl Firmen, und neben Palantir kennt man drei davon im Wissenschaftsbereich schon sehr lange: RELX, Thomson Reuters und Clarivate. *Paranoid computing* hat sich demnach teils auch aus dem Wissenschaftsbereich heraus entwickelt, teils durch die Vielzahl von Aufkäufen, durch Fusionen und die Erschließung neuer Geschäftsfelder sich dort festgesetzt – und mit Scoring kennt man sich im Wissenschaftsbereich ebenso schon lange aus. Wie sehr entsprechende Mentalitäten verankert sind, zeigt z.B. die Aufzeichnung des Webinars der Scholarly Network Security Initiative (SNSI), die vor einiger Zeit Furore machte,[5] worin frühere FBI-Angehörige von *bad actors* raunen. Gefahren, gegen die man sich wappnen müsse, seien überall.[6]

Nun haben mindestens die verschiedenen Ransomware-Attacken auf Hochschulen und Kliniken der letzten Zeit gezeigt, dass es tatsächlich Gefahren gibt. Aber für deren Bekämpfung sind andere zuständig als die Plattformen des paranoid computing, die selbst eine lange Geschichte gehackter Daten haben, wie McKenzie Funk zeigen kann. (vgl. S. 143ff.) Noch mehr wäre aber unter der Perspektive von digitaler Souveränität zu fragen, ob wir paranoid computing eigentlich weiterhin beeinflussen lassen wollen, welche Fragen die Wissenschaft stellen kann? Was für Methoden verwendet werden, wer mit wem zusammenarbeitet, wer welche Daten sehen kann? Palantir, das zuletzt mit KI-getriebenen Tötungssystemen Aufsehen erregte,[7] hat sich u.a. in Großbritannien die Gesundheitsdaten schon zu eigen gemacht[8] und interessiert sich Gerüchten zufolge lebhaft für die deutsche Nationale Forschungsdateninfrastruktur. LexisNexis dringt auch in Europa in den Markt der Mobilitätsdaten ein.[9] Haben wir diese Entwicklungen im Blick? Und wenn wir in den Infrastrukturen des paranoid computing arbeiten und unsererseits Identifier vergeben, normieren, zuordnen – sind wir dann sicher oder naiv, dass wir dabei nicht als *Mechanical Turks* eine eigene Gattung von »Dual Use«-Gütern produzieren und die digitalen Akten unserer Nutzenden füllen helfen, die noch weniger als wir überblicken, was wir da eigentlich tun?

Die europäische Datenstrategie war ursprünglich auch, in Reaktion auf die internationalen Entwicklungen, darauf aufgebaut, zunächst die Rechte der Bürgerinnen und Bürger zu sichern, bevor im

4 Vgl. Data fusion market size and forecast, https://www.verifiedmarketresearch.com/product/data-fusion-market/, Data fusion market insights research report [2023-2030], Linkedin 12.12.2023, https://www.linkedin.com/pulse/data-fusion-market-insights-research-report-2023-2030-fdslf, Stand: 20.02.2024.

5 Vgl. Leonhard Dobusch: Kein Open-Access-Deal, dafür mit Spyware gegen Schattenbibliotheken? Netzpolitik, 26.10.2020, https://netzpolitik.org/2020/neues-vom-grossverlag-elsevier-kein-open-access-deal-dafuer-mit-spyware-gegen-schattenbibliotheken/; Mehta, Gautama: Proposal to install spyware in university libraries to protect copyrights shocks academics, coda, 13.11.2020, https://www.codastory.com/authoritarian-tech/spyware-in-libraries/, Stand: 20.02.2024.

6 Vgl. David Tucker: SNSI webinar, https://vimeo.com/623425480, Stand: 20.02.2024.

7 Vgl. Bergengruen, Vera: How tech giants turn Ukraine in an ai war lab, Time, 08.02.2024, https://time.com/6691662/ai-ukraine-war-palantir/; Kreye, Andrian und Mascolo, Georg: Wisch und weg. KI im Krieg, Süddeutsche Zeitung, 27.05.2023, https://www.sueddeutsche.de/projekte/artikel/kultur/ki-und-krieg-palantir-ukraine-e666421/?reduced=true, Stand 20.02.2024.

8 Vgl. Koch, Marie-Claire: eHealth: Umstrittenes Unternehmen Palantir gewinnt größten Datendeal Englands, heise online, 23.11.2023, https://www.heise.de/news/eHealth-Umstrittenes-Unternehmen-Palantir-gewinnt-groessten-Datendeal-Englands-9537039.html, Stand: 20.02.2024.

9 Vgl. LexisNexis Risk Solutions wurde für das EU-Konsortium Horizon 2020 ausgewählt, PR Newswire, 04.11.2020, https://www.prnewswire.com/news-releases/lexisnexis-risk-solutions-wurde-fur-das-eu-konsortium-horizon-2020-ausgewahlt-817539385.html, Stand: 20.02.2024.

europäischen Binnenmarkt Daten getauscht werden und darüber Wertschöpfung und gesellschaftlicher Nutzen entstehen können. Das ist die Rolle der Datenschutzgrundverordnung, die auch von amerikanischen Lobbyisten wütend bekämpft wurde, bis sie in der historischen Schrecksekunde der Snowden-Enthüllungen doch verabschiedet werden konnte. Dieser Weg eines Ausgleichs von Datenökonomie und freiheitlicher Gesellschaft droht immer wieder verloren zu gehen. Datenschutz soll jetzt »ermöglichend« sein und der »Innovation nicht im Weg« stehen. Als würden beim Datenschutz Einsen und Nullen geschützt werden und eben nicht Menschen, an die McKenzie Funk in diesem Buch erinnert. Und so wie dieses Buch mit einer höflichen Vorstellung begann, endet es daher mit einem freundlichen Dank:

„To the many brave and generous people who sat down with me or answered the phone when I called: thank you. It was an act of faith. To those who didn't dare: I understand. Maybe you thought I would get the story wrong. Maybe you thought I would get it right. There are reasons, in this world, to be afraid of both." (S. 251)

Renke Siems, Ministerium für Wissenschaft, Forschung und Kunst Baden-Württemberg, Stuttgart

Zitierfähiger Link (DOI): https://doi.org/10.5282/o-bib/6201