H 7625

FIfF Kommunikation

Zeitschrift für Informatik und Gesellschaft

36. Jahrgang 2019 Einzelpreis: 7 EUR

4/2019 – Dezember 2019

ISSN 0938-3476

• Überwachungs-Gesamtrechnung • Gegen Antisemitismus • Netzpolitik •

FIfF Kommunikation

Zeitschrift für Informatik und Gesellschaft

Titelbild: Salomé von Sebastian Hertrich,
Foto: Anna Franke. Siehe dazu auch Seite 6.

Inhalt

Ausgabe 4/2019

inhalt

Editorial

Es ist ein Meilenstein in der Geschichte unseres Engagements gegen die staatliche Telekommunikationsüberwachung: Im Jahr 2010 erklärte das Bundesverfassungsgericht die Umsetzung der EU-Richtlinie 2006/24/EG – die *Vorratsdatenspeicherung* – in den §§ 113 a und 113 b des Telekommunikations-Gesetzes für nichtig (1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08). Die Verfassungswidrigkeit dieser Regelung wurde damit höchstrichterlich bestätigt.

Das Richtergebäude des Bundesverfassungsgerichts
Foto: Rainer Lück, CC BY-SA 3.0 de

Trotz dieses eindeutigen Urteils ist nach der Ansicht des Bundesverfassungsgerichts jedoch nicht jede Speicherung von Telekommunikationsdaten per se verboten. Verboten ist „… eine Sammlung von personenbezogenen Daten auf Vorrat zu unbestimmten oder noch nicht bestimmbaren Zwecken …“ (Rn. 213). Weiter: „Die Einführung der Telekommunikationsverkehrsdatenspeicherung kann … nicht als Vorbild für die Schaffung weiterer vorsorglich anlassloser Datensammlungen dienen, sondern zwingt den Gesetzgeber bei der Erwägung neuer Speicherungspflichten oder -berechtigungen in Blick auf die Gesamtheit der verschiedenen schon vorhandenen Datensammlungen zu größerer Zurückhaltung. … Durch eine vorsorgliche Speicherung der Telekommunikationsverkehrsdaten wird der Spielraum für weitere anlasslose Datensammlungen auch über den Weg der Europäischen Union erheblich geringer“ (Rn. 218). Die Überwachungsmaßnahmen müssen nach der Rechtsprechung des Bundesverfassungsgerichts also in ihrer Gesamtheit gesehen werden – das ist die *Überwachungs-Gesamtrechnung*, der wir den Schwerpunkt in dieser Ausgabe widmen, den *Dagmar Boedicker* gestaltet hat. „Wir sind nicht nur einem der vielen Gesetze in der Sicherheits-Architektur, oder nur einer Sicherheitsbehörde unterworfen, sondern vielen“, schreibt sie dazu einleitend. „Niemand weiß, welche Sicherheitsbehörde auf Basis welchen Gesetzes wann welche privaten Daten abgreifen darf. Eigentlich ein verfassungswidriger Zustand.“ Im Schwerpunkteditorial ab Seite 19 leitet sie den Schwerpunkt ein und gibt einen Überblick über dessen Beiträge.

Doch die nächste Überwachungsmaßnahme kommt schon um die Ecke: Die *E-Evidence-Verordnung* der EU, gegen die wir in einem offenen Brief gemeinsam mit zwölf weiteren Bürgerrechtsorganisationen Stellung beziehen. „Mit der Verordnung könnten nationale Strafverfolger EU-weit Provider zwingen, Daten herauszugeben – ohne dass das Land, in dem der Provider sitzt oder die Daten gespeichert sind, mitentscheidet“, heißt es in der gemeinsamen Pressemitteilung. „Der Vorschlag nimmt Staaten die Möglichkeit, die Grundrechte ihrer Bürger zu schützen. Er höhlt das europäische Datenschutzrecht aus und droht, das bestehende internationale System der Rechtshilfe in Strafsachen zu beschädigen“, so das Schreiben selbst. Pressemitteilung und offener Brief sind in dieser Ausgabe dokumentiert.

Die Politik in Deutschland rückt nach rechts. Dies machen das Aufkommen rechtspopulistischer und rechtsextremistischer Parteien und ihr Einzug in Parlamente, aber auch verschiedentliche Einlassungen aus „staatstragenden“ konservativen Parteien deutlich. Falls es noch eines Beweises bedurft hätte: Gerade wurde der antifaschistischen *Vereinigung der Verfolgten des Naziregimes* von der Berliner Finanzverwaltung die Gemeinnützigkeit aberkannt.

Der Antisemitismus mit seinen schrecklichen Folgen war die Basis der nationalsozialistischen Herrschaft. Kompromisslos gegen den in manchen Kreisen heute wieder aufkommenden Antisemitismus bezieht *Klaus Fuchs-Kittowski* Stellung. „Warum gehen erwachsene Männer aus rassistischen Gründen gewaltsam gegen Kinder und Jugendliche vor? Hier hat unsere Gesellschaft, hier hat Berlin, haben wir ein ernsthaftes Problem!“ Er sieht die Wissenschaft in der Verantwortung: Die Forderung muss sein, „… dass sie ihre Verantwortung wahrnimmt: die Wahrheit ihrer Aussagen zu sichern und eine dem Leben, dem Menschen dienliche Anwendung der Wahrheit zu realisieren und somit auch darin ihre Verantwortung sieht, eine tiefe ‚Wahr-Nehmung‘ des Lebens und des Menschen zu befördern, nicht zu behindern, sodass die Natur und der Mensch in ihrer Spezifik und ihrem Wert erkannt und anerkannt werden.“ Der Imperativ lautet: „Die Wissenschaft soll der Förderung der Menschenrechte dienen.“ Klaus Fuchs-Kittowski entwickelt diese Forderung anhand einer Reihe von Aspekten und bezieht sich dabei auch auf die Geschichte der Diskussion zur wissenschaftlichen Verantwortung, die er selbst mit geprägt hat. Es kann keinen Zweifel geben: „Es muss gewährleistet werden, dass Juden sich überall in Deutschland angstfrei bewegen und zu erkennen geben können. Dazu muss die Zivilgesellschaft aufgerüttelt werden und die Verbrecher auch strafrechtlich belangt werden. Das schulden wir: ‚Den 6 Millionen, die keine Retter fanden.‘“

Am 12. Oktober 2019 starb *Wolf-Dieter Narr*, Professor am Otto-Suhr-Institut der Freien Universität Berlin. Wir gedenken seiner mit einem Nachruf, den *Elke Steven* verfasst hat.

In unserer Rubrik *Netzpolitik*, für deren Beiträge wir *netzpolitik.org* herzlich danken, haben wir diesmal die Schwerpunkte Arbeitnehmerdatenschutz – in einem Interview mit *Peter Wedde* – und die Arbeit der *Datenethikkommission* gesetzt. Es lohnt sich sicherlich, auch deren Abschlussbericht zu lesen.

Zwei Rezensionen runden die Ausgabe ab: *Dietrich Meyer-Ebrecht* hat sich die Biographie *Permanent Record* von Edward Snowden vorgenommen und *Stefan Hügel* hat den Sammelband *Information Technology for Peace and Security* rezensiert, der von Christian Reuter, Professor am Institut PEASEC der Technischen Universität Darmstadt, herausgegeben wurde.

Gerade ist unsere diesjährigen FIfF-Konferenz – Künstliche Intelligenz als Wunderland – zu Ende gegangen, die in diesem Jahr vom Organisationsteam aus Bremen ausgerichtet wurde – herzlichen Dank an dieser Stelle für eine großartige Konferenz. *Hans-Jörg Kreowski* hält eine kurze Rückschau darauf; den ausführlichen Bericht mit den Beiträgen der Referentinnen und Referenten und der diesjährigen Verleihung des Weizenbaum-Studienpreises wird es in der nächsten Ausgabe geben.

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

Stefan Hügel
für die Redaktion

Der Brief

Verantwortung

Liebe Leserinnen und Leser, liebe Mitglieder des FIfF,

vor vierzig Jahren, 1979, veröffentlichte der Philosoph Hans Jonas das Buch *Das Prinzip Verantwortung*, in dem er eine neue Ethik für die technologische Zivilisation fordert. Er leitet seine Analyse ein mit der Feststellung:

> *„Der endgültig entfesselte Prometheus, dem die Wissenschaft nie gekannte Kräfte und die Wirtschaft den rastlosen Antrieb gibt, ruft nach einer Ethik, die durch freiwillige Zügel seine Macht davor zurückhält, dem Menschen zum Unheil zu werden."*[1]

Jonas leitete daraus seinen bekannten Imperativ ab:

> *„Handle stets so, dass die Wirkungen Deiner Handlung verträglich sind mit der Permanenz echten menschlichen Leben auf Erden"*[2],

oder, anders formuliert:

> *„Schließe in Deine gegenwärtige Wahl die zukünftige Integrität des Menschen als Mit-Gegenstand Deines Wollens ein."*[3]

Zweifellos kann man bereits diese Forderung von zwei Seiten hinterfragen: Soll wirklich die Permanenz *menschlichen* Lebens die Maxime unseres Handelns sein? Und: Soll es dabei *ausschließlich* um die Permanenz menschlichen Lebens gehen? Die erste Frage ist bei Hans Jonas als Axiom gesetzt und wird nicht in Frage gestellt. Bei der zweiten spielen sicherlich auch persönliche Wertvorstellungen eine Rolle; zweifellos gibt es hier auch Abhängigkeiten.

Eine der größte Gefährdungen, die dem Leben auf Erden derzeit droht, ist der Klimawandel. Manche vertrauen auf die Selbstheilungskräfte der Natur und halten Maßnahmen gegen den Klimawandel für überflüssig. Dies würde bedeuten, dass menschliches Leben einem abstrakten Verständnis von Natur untergeordnet wäre – ist es doch völlig unklar, ob in einer solchen, „selbstgeheilten" Natur für den Menschen noch Platz wäre. „Die Natur braucht uns nicht – aber wir brauchen die Natur." Manche mögen sich noch an diesen Spruch aus dem Fernsehen der 80-er Jahre – ich kenne ihn aus dem damaligen Baden-Württembergischen Regionalprogramm – erinnern. Ähnlich die fatalistische Ansicht, wir könnten gegen den Klimawandel ohnehin nichts unternehmen, da er nicht menschengemacht sei. Ich bin da optimistischer: Gerade *weil* der Klimawandel menschengemacht ist, können wir noch etwas dagegen tun.

Hier kommt der Imperativ von Hans Jonas ins Spiel: Wir müssen die Verantwortung dafür übernehmen, den Klimawandel zu stoppen und die dafür erforderlichen Maßnahmen zu ergreifen. Das Übereinkommen von Paris macht unmissverständlich klar, dass wir uns der Gefahr bewusst sind und die Ziele kennen, die wir erreichen müssen, um sie abzuwenden – vereinfacht geschrieben: die Erderwärmung auf maximal 1,5°C zu begrenzen.

Offensichtlich werden die dafür erforderlichen Maßnahmen immer drastischer, je länger wir damit warten. Um also einen sozialverträglichen Übergang in eine klimagerechte Wirtschaft und Politik zu erreichen, müssen wir schnell handeln. Greta Thunberg betonte auf der UN-Klimakonferenz in Katowice:

> *„What I hope we achieve at this conference is that we realise that we are facing an existential threat. This is the biggest crisis humanity has ever faced. First we have to realise this and then as fast as possible do something to stop the emissions and try to save what we can save."*[4]

Wie gehen wir nun damit um? Dies ist zunächst der eindringliche Appell, Menschen, die angesichts der eindeutigen Feststellungen der Wissenschaft[5] und der heute schon eindeutig dem Klimawandel zurechenbaren Wetterereignisse[6] immer noch behaupten, es gäbe keinen Klimawandel, endlich nicht mehr ernst zu nehmen. Darauf folgt das klare Verständnis, was der Klimawandel für uns und für die gesamte Menschheit bedeutet: Extreme Wetterereignisse, der absehbare Anstieg des Meeresspiegels mit den Folgen, die dies für viele Regionen und ihre BewohnerInnen hat, und in der Folge klimabedingte Kriege und

klimabedingte Migration. Selbstverständlich können wir gleichzeitig auch auf einen wissenschaftlichen Fortschritt hoffen, der die Folgen des Klimawandels reduzieren hilft. Einige Ergebnisse dieses wissenschaftlichen Fortschritts sehen wir sogar schon heute: beispielsweise Sonnenenergie durch Photovoltaik oder Windkraft[7]. Warum aber wenden wir diese Möglichkeiten, die uns der technische Fortschritt heute schon bietet, nicht konsequent an? Stattdessen verfeuern wir weiter Kohle[8] und schwadronieren über „Flugtaxis"[9] – eine Technologie deren allgemeine Anwendbarkeit bestenfalls weit in der Zukunft liegt.

Zurück zum Ausgangsthema: Was bedeutet es heute, Verantwortung zu übernehmen? In der öffentlichen Debatte erleben wir schon längst eine Bedeutungsverschiebung. Sagt jemand: „Deutschland muss in der Welt wieder Verantwortung übernehmen", bedeutet dies in der Regel eben nicht, das wir beispielsweise stärker dazu beitragen müssen, den Klimawandel zu verlangsamen oder zu verhindern. Im Gegenteil: Hier wird stets betont, dass wir ohne „die anderen" ohnehin nichts tun könnten. Nein: Mit solch einer Aussage ist meist die Erwartung verbunden, in Krisengebieten Frieden herbeibomben zu können. „Verantwortung zu übernehmen" bedeutet in der heutigen politischen Rhetorik: Militärisch zu intervenieren.

Welche Rolle dabei Menschenrechte spielen, ist mindestens unklar. Als 2011 der mutmaßliche Terrorist Osama Bin Laden von einem US-amerikanischen Militärkommando niedergeknallt wurde[10], betonte der Journalist Jörg Schönenborn noch:

> *„Mein Verständnis von einem Rechtsstaat ist es nicht, dass Mörder einfach abgeknallt werden."*[11]

Die Bundeskanzlerin sah das anders und sagte:

> *„Ich freue mich darüber, dass es gelungen ist, Bin Laden zu töten."*[12]

Schon dies zeigt die unterschiedlichen Wertvorstellungen in unserer Gesellschaft. Als nun der mutmaßliche Terrorist Abu Bakr al-Baghdadi auf ähnliche Weise getötet wurde[13], hat man sich anscheinend mit menschenrechtlichen Kinkerlitzchen gar nicht mehr aufgehalten.

Der letzte Begriff von Verantwortung spielt sich wieder in Deutschland ab, genauer: in Bayern. Auf niedere Instinkte vertraute die CSU bei der Bundestagswahl 2013, als sie eine PKW-Maut „für Ausländer" in Aussicht stellte. Dass es ein kleines Problem mit EU-Recht geben könnte, wurde ebenso wie das entsprechende Gutachten des wissenschaftlichen Dienstes des Deutschen Bundestages ignoriert und vom Tisch gewischt. Eilig wurden die entsprechenden Verträge mit privaten[14] Anbietern geschlossen. Nach dem (absehbar) ablehnenden Urteil des EuGH werden sich nun die Kosten für den Steuerzahler im dreistelligen Millionenbereich bewegen. Wer wird wohl dafür die „Verantwortung" übernehmen?

Das Fazit ist banal: Menschen müssen Verantwortung übernehmen und Entscheidungen treffen. Sie müssen dieser Verantwortung gerecht werden – und das heißt auch: Sie müssen gegebenenfalls auch persönlich die Konsequenzen dafür tragen. Häufig sind politische Fragestellungen komplexer, als sie sich in der Öffentlichkeit darstellen – viele unterschiedliche Interessen müssen zum Ausgleich gebracht werden, viele Parameter sind zu bedenken. Das darf aber nicht dazu führen, nichts zu tun. Wir brauchen mehr Transparenz: Wo werden welche Entscheidungen getroffen, welche Einflüsse gibt es, wie werden sie gewichtet. Der Eindruck, dass politische Entscheidungen vor allem durch wirtschaftlich starke Akteure auf Kosten der jungen Generation getroffen werden, ist fatal. Schon immer gab es Generationenkonflikte zwischen den Jüngeren und den Älteren. Der Vorwurf, nach dem Prinzip „Nach mir die Sintflut" zu verfahren, ist nicht neu. Doch heute geht es um mehr: Von den politischen Entscheidungen der nächsten Jahre könnte wirklich der Fortbestand des menschlichen Lebens abhängen. Der Imperativ von Hans Jonas ist vielleicht so aktuell wie noch nie.

Mit FIfFigen Grüßen

Stefan Hügel

Anmerkungen

1 *Jonas H (1979) Das Prinzip Verantwortung. Versuch einer Ethik für die technologische Zivilisation. Frankfurt am Main: suhrkamp, S. 7*
2 *Jonas H (1979), a. a. O., S. 36*
3 *ebd.*
4 *zit. nach Wikipedia, Stichwort Greta Thunberg, https://de.wikipedia.org/wiki/Greta_Thunberg, Abruf 10. November 2019*
5 *nur stellvertretend: Scientists for Future, https://scientists4future.org*
6 *Die Zuordung von Wetterereignissen unternimmt die Attributionswissenschaft. Wenn man in diesem Jahr ein einziges Buch gelesen hat, sollte es vielleicht dieses sein: Otto F (2019) Wütendes Wetter. Auf der Suche nach den Schuldigen für Hitzewellen, Hochwasser und Stürme. Berlin: Ullstein*
7 *vgl. Quaschning V (2018) Erneuerbare Energien und Klimaschutz. Hintergründe, Techniken und Planung, Ökonomie und Ökologie, Energiewende. München: Hanser*
8 *„Datteln 4" im Ruhrgebiet: Kohlekraftwerk soll wohl doch ans Netz. Frankfurter Allgemeine, https://www.faz.net/aktuell/wirtschaft/klima-energie-und-umwelt/kohlekraftwerk-datteln-4-soll-wohl-doch-ans-netz-16459851.html*
9 *CSU-MinisterInnen stellen Flugtaxi vor: Der erste Testflug ist geschafft. taz, https://taz.de/CSU-MinisterInnen-stellen-Flugtaxi-vor/!5576436/*
10 *Owen M (2012) No easy day. The only first-hand account of the Navy Seal Mission that killed Osama Bin Laden. London: Penguin Books*
11 *Ich zitierte dies damals im „Brief": Brief an das FIfF: Ethik und Zivilisation. FIfF-Kommunikation 2/2011*
12 *Freude über Bin Ladens Tod: Wie ein Richter Merkel zur Räson bringen will. Spiegel Online, https://www.spiegel.de/panorama/justiz/freude-ueber-bin-ladens-tod-wie-ein-richter-merkel-zur-raeson-bringen-will-a-761166.html.*
13 *Donald Trump bestätigt Tod des IS-Führers Abu Bakr al-Baghdadi. Spiegel Online, https://www.spiegel.de/politik/ausland/abu-bakr-al-baghdadi-donald-trump-bestaetigt-tod-des-is-fuehrers-a-1293551.html. Scheinbar hat US-Präsident Trump ihn zusätzlich verhöhnt, als er seinen Tod bekannt gab. Speigel Online konzentrierte sich vor allem auf die Frage, ob die Tötung Donald Trump politisch helfe.*
14 *Erich Fromm weist darauf hin, dass der lateinische Begriff „privare" für „berauben" steht: Fromm E (1976) Haben oder Sein. Die seelischen Grundlagen einer neuen Gesellschaft. 22. Aufl. 1993, Stuttgart: dtv, S. 73*

Sebastian Hertrich

Salomé

Was sie uns sagen kann

Die Darstellung der Salomé ist inspiriert durch das Drama von Oscar Wilde. Dort ist sie die Stieftochter des Herodes. Herodes fordert von ihr einen Schleiertanz und verspricht ihr jegliche Gegenleistung. Salomé willigt ein und fordert wiederum als Gegenleistung die Enthauptung Johannes des Täufers, den Herodes gefangen hält.

Die Salomé in der Kombination aus geschnitztem Plexiglas und einem Gewand aus Computerplatinen ist eine Allegorie der Digitalität: Wir wünschen uns von ihr die Erfüllung unserer Träume, doch dafür fordert sie im Gegenzug außerordentliche Opfer, ob Ressourcen in Form von Energie und Rohstoffen oder Zeit und Nerven, die wir im Umgang mit ihr zur Verfügung stellen müssen.

Salomés Geste ist eine gewollte Verschmelzung aus Mahnung zur Vorsicht und der Aufforderung zum Schweigen. Beides bezieht sich auf teils negative Entwicklungen der Digitalisierung, deren Folgen wir noch nicht voll erfassen können, sei es die wachsende Überwachung einzelner Bürger und die damit einhergehende Kontrolle, seien es ihr Verstärken marktwirtschaftlicher Mechanismen oder ihr Einfluss auf soziale Einrichtungen wie Krankenkassen oder die Bildung.

Wir opfern ihr ebenfalls unsere Spiritualität in der Hoffnung, sie für rationale Erklärungen einzutauschen – oder für einen kurzen Moment der Lust und Erregung.

Sebastian Hertrich ist Holzbildhauer und Diplomkünstler in Erlangen.

13 zivilgesellschaftliche Organisationen

Kein grenzüberschreitender Direktzugriff auf Daten

13 Organisationen warnen in offenem Brief vor E-Evidence-Verordnung

13 zivilgesellschaftliche Organisationen wenden sich in einem offenen Brief an die deutschen Abgeordneten im EU-Parlament, um vor der E-Evidence-Verordnung zu warnen. Sie fordern zunächst eine Evaluation der Europäischen Ermittlungsanordnung.

Mit der E-Evidence-Verordnung könnten nationale Strafverfolger EU-weit Provider zwingen, Daten herauszugeben –, ohne dass das Land, in dem der Provider sitzt oder die Daten gespeichert sind, mit entscheidet. Zum Beispiel müssten Anbieter von E-Mail- oder Messenger-Diensten Verbindungsdaten und sogar Inhalte von Nachrichten herausgeben. Dabei ist nicht erforderlich, dass die Tat, wegen der ermittelt wird, überhaupt eine Straftat in dem Staat ist, in dem der Provider sitzt oder in dem der Beschuldigte lebt.

„Der Vorschlag nimmt Staaten die Möglichkeit, die Grundrechte ihrer Bürger zu schützen. Er höhlt das europäische Datenschutzrecht aus und droht, das bestehende internationale System der Rechtshilfe in Strafsachen zu beschädigen," heißt es in dem Schreiben.

Die Organisationen kritisieren weiter, dass politische Verfolgung über Staatsgrenzen hinweg durch den Verzicht auf beidseitige Strafbarkeit erleichtert wird. „Wenn eine Tat in einem Staat legal ist, dann dürfen dort ansässige Provider nicht gezwungen werden, Beweismittel über solche Vorgänge herauszugeben," sagt Elisabeth Niekrenz, politische Referentin von *Digitale Gesellschaft e. V.*

Auch Berufsgeheimnisse und Zeugnisverweigerungsrechte werden nicht geschützt. So können anwaltliche, journalistische oder ärztliche Tätigkeiten betroffen sein. „Die Verhandlungen über ein Partnerschaftsabkommen mit den USA führen im schlimmsten Fall zur Echtzeit-Überwachung unserer Online-Kommunikation durch die Ermittlungsbehörden. Presse- und Meinungsfreiheit sind gefährdet", so Alexander von Gernler, Vizepräsident der Gesellschaft für Informatik e. V. (GI).

„Die E-Evidence-Verordnung wäre toxisch für die Rechtsstaatlichkeit in der EU", sagt Friedemann Ebelt von *Digitalcourage*. „Das gilt insbesondere in Kombination mit flächendeckender Vorratsdatenspeicherung und dem derzeitigen Wettbewerb zur Einschränkung von Grundrechten, den sich die Regierungen der EU-Länder aktuell liefern."

Vieles spricht gegen die Notwenigkeit der Verordnung: Mit der Europäischen Ermittlungsanordnung schuf die EU erst vor wenigen Jahren ein Instrument, das grenzüberschreitende Strafverfolgung erleichtert. Eine Evaluation fand bis heute nicht statt.

Nachdem die Kommission den Entwurf zur E-Evidence-Verordnung im April 2018 auf den Weg gebracht hatte, votierte Deutschland im Dezember 2018 dagegen, wurde aber überstimmt. Derzeit erarbeitet der Ausschuss des europäischen Parlaments für Bürgerliche Freiheiten, Justiz und Inneres (LIBE) einen Bericht. Währenddessen hat die Kommission bereits Verhandlungen mit den USA über ein Partnerschaftsabkommen gestartet. Damit übergeht sie das Parlament, das sich noch nicht auf einen Standpunkt festgelegt hat.

Der offene Brief im Wortlaut

AN:
Die deutschen Abgeordneten des Europäischen Parlaments

Berlin, 23.10.2019

Betreff: Kein grenzüberschreitender Direktzugriff auf persönliche Daten

Sehr geehrte Damen und Herren,

das Europäische Parlament berät über die Vorschläge von Kommission und Rat zu einer geplanten Verordnung über elektronische Beweismittel. Wir wenden uns an Sie, um unserer Besorgnis über den Vorschlag Ausdruck zu verleihen.

Der Entwurf sieht vor, dass Strafverfolgungsbehörden eines Mitgliedstaates (Anordnungsstaat) Provider, die in einem anderen Mitgliedstaat ansässig sind (Vollstreckungsstaat), unmittelbar verpflichten können, Meta- und Inhaltsdaten ihrer Kunden herauszugeben. Die Herausgabe muss binnen zehn Tagen und in Notfällen binnen 6 Stunden erfolgen. Halten sich Anbieter nicht daran, so drohen ihnen Sanktionen in Höhe von bis zu 2 % des weltweiten Jahresumsatzes. Der Vollstreckungsstaat muss die Anordnung nicht auf ihre Rechtmäßigkeit hin überprüfen und hat kein Recht, ihr zu widersprechen. Er ist hingegen verpflichtet, bei Nichteinhaltung eine Sanktion gegenüber dem Provider zu verhängen und zu vollstrecken. Dabei ist nicht erforderlich, dass die Tat, wegen der ermittelt wird, in beiden Staaten eine Straftat ist. Auch Anbieter, die in Drittstaaten sitzen, in denen die zu verfolgende Tat keine Straftat ist, sollen zur Datenherausgabe verpflichtet werden dürfen, wenn sie ihre Dienste in der Europäischen Union anbieten.

Die unterzeichnenden Organisationen warnen ausdrücklich vor diesem Vorhaben. Der Vorschlag nimmt Staaten die Möglichkeit, die Grundrechte ihrer Bürger zu schützen. Er höhlt das europäische Datenschutzrecht aus und droht, das bestehende internationale System der Rechtshilfe in Strafsachen zu beschädigen. Nur zwei Jahre nach Ablauf der Umsetzungsfrist der europäischen Ermittlungsanordnung ist nicht geklärt, ob tatsächlich Lücken in der grenzüberschreitenden Strafverfolgung bestehen.

Unten finden Sie unsere Kritikpunkte im Einzelnen.

Mit freundlichen Grüßen

Chaos Computer Club e. V., Deutsche Vereinigung für Datenschutz e. V., digitalcourage e. V., Digitale Freiheit, Digitale Gesellschaft e. V., Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e. V., Gesellschaft für Informatik e. V., Humanistische Union e. V., Neue Richtervereinigung e. V. Organisationsbüro der Strafverteidigervereinigungen, Republikanischer Anwältinnen- und Anwälteverein e. V. SaveTheInternet, Vereinigung Demokratischer Juristinnen und Juristen e. V.; Als Einzelperson: Kilian Vieth, Stiftung Neue Verantwortung

Unsere Kritikpunkte im Einzelnen:

Der Grundrechtsschutz kann nicht sichergestellt werden

Der vollstreckende Staat hat keine Möglichkeit, für die Einhaltung des grundgesetzlich vorgeschriebenen Schutzes zu sorgen.

1. In welchen Fällen eine Datenherausgabe möglich ist, richtet sich ausschließlich nach dem Recht des Anordnungsstaats. Dadurch ist es möglich, dass Ermittlungsbehörden aus anderen europäischen Ländern unter niedrigeren Voraussetzungen Daten aus Deutschland erhalten können, als dies deutschen Behörden möglich wäre. Dies bedeutet eine Aushöhlung der Regelungen der Strafprozessordnung und der Rechtsprechung des Bundesverfassungsgerichts zum Schutz des Grundrechts auf informationelle Selbstbestimmung.

2. Der Vollstreckungsstaat kann den Schutz von Berufsgeheimnisträgern, Immunitäten und Zeugnisverweigerungsrechten oder die Verhältnismäßigkeit einer Datenverarbeitung nicht sicherstellen. Die vom Rat eingefügte Notifikation stellt keine ausreichende Schutzmöglichkeit dar, da der Vollstreckungsstaat lediglich Hinweise auf die Betroffenheit von Immunitäten oder Berufsgeheimnisträgern geben kann, aber kein Recht zur verbindlichen Ablehnung besteht. Selbst gegen eine offensichtlich missbräuchliche Anordnung steht dem Vollstreckungsstaat kein Veto-Recht zu.

Ohne beidseitige Strafbarkeit ist politische Verfolgung möglich

Das Strafrecht ist in den Staaten der europäischen Union nicht harmonisiert. Was als Straftat gilt und was nicht, differiert stark. So reichen in etwa die Gesetze über die Strafbarkeit von Schwangerschaftsabbrüchen von einem umfassenden Verbot (Malta) bis hin zu weitgehender Liberalisierung wie in den Niederlanden. In Polen ist es eine Straftat, der polnischen Bevölkerung oder dem polnischen Staat eine Mitverantwortung für den Holocaust zu geben. Auch bezüglich der Verletzung des Bankgeheimnisses und vieler anderer Tatbestände bestehen erhebliche Unterschiede, wie erst vor wenigen Jahren an dem pro-

minenten Fall *Puigdemont* deutlich wurde. Mit der E-Evidence werden Anbieter und Staaten gezwungen, an der Verfolgung von Taten mitzuwirken, die in ihrem Land legal sind. Dies wird auch zu politisch ungewollten Ergebnissen führen.

Die Erforderlichkeit des Instruments ist nicht belegt

Erst 2014 hat das Europäische Parlament die Richtlinie über die Europäische Ermittlungsanordnung verabschiedet, die eine schnellere Zusammenarbeit der Strafverfolgungsbehörden ermöglichen soll. Sie schafft verbindliche Fristen für die grenzüberschreitende Kooperation. Die Umsetzungsfrist ist erst 2017 ausgelaufen. Eine Evaluation fand noch nicht statt. Es gibt keine Studien darüber, welchen Beitrag die europäische Ermittlungsanordnung zur Gewinnung elektronischer Beweismittel leistet, ob Verbesserungsbedarf besteht und wo eventuelle Schwächen liegen. Auch Erkenntnisse darüber fehlen, in wie vielen Fällen Ermittlungen eingestellt werden mussten, weil der Zugriff auf elektronische Daten nicht möglich war. Ohne Erkenntnisse über die Wirksamkeit erst kürzlich etablierter Instrumente ist die Einführung eines neuen Regelwerks unverhältnismäßig. Wir fordern eine evidenzbasierte Sicherheitspolitik.

Ein internationaler *Spill-Over*-Effekt ist zu befürchten, der politische Verfolgung erleichtern wird

Die internationale Zusammenarbeit in Strafsachen ist bisher durch gegenseitige Rechtshilfe geprägt. Von der E-Evidence-Verordnung sind auch Dienste mit Sitz in Drittstaaten betroffen, die Daten außerhalb der EU speichern. Wenn die EU einseitig Regeln aufstellt, die in anderen Staaten gelten sollen, bricht sie mit dem Konzept der gegenseitigen Rechtshilfe. Dies wird Drittstaaten einladen, ähnlich zu verfahren. Autoritäre Staaten können ebenso international tätige Anbieter verpflichten, in der Europäischen Union gespeicherte Daten herauszugeben. Damit werden politisch Verfolgte, die im Ausland Schutz suchen, gefährdet. Zudem werden die Wertungen der Datenschutzgrundverordnung ausgehöhlt: Sie verlangt von Datenverarbeitern, Daten, die in der EU gespeichert sind, nur unter sehr engen Voraussetzungen in Drittstaaten zu übertragen. Die E-Evidence nimmt aber keine Rücksicht darauf, ob nationale Datenschutzgesetze von Drittstaaten eine Übertragung in die EU gestatten.[1]

Der Bundesrat befürchtet in seiner Stellungnahme eine „Erosion der bisherigen und bewährten Prinzipien der Rechtshilfe und des international arbeitsteiligen Strafverfahrens".[2]

Die bereits begonnenen Verhandlungen der Kommission mit den USA übergehen das Parlament

Die Kommission hat bereits Verhandlungen mit den USA über ein Kooperationsabkommen begonnen, bevor das Parlament sich einen Standpunkt zur diesem Abkommen zugrundeliegende E-Evidence-Verordnung bilden konnte. Damit wird nicht nur das Parlament als direkt demokratisch legitimierte Institution der EU übergangen. Die USA haben den Rahmen für ein solches Abkommen durch ein 2018 verabschiedetes Gesetz, den *CLOUD-Act*, bereits vorgegeben. Vieles spricht dafür, dass ein Abkommen, das den Anforderungen der DSGVO und des CLOUD-Act gerecht wird, nicht möglich ist.

Anmerkungen

1 *Vgl. Böse, An Assessment of the Commission's proposal on electronic evidence, Study requested by the LIBE committee, September 2018, S. 35.*

2 *Bundesrat, Drucksache 215/18, Beschluss vom 06.07.2018: Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen, S. 11.*

Klaus Fuchs-Kittowski

Gegen Antisemitismus

Zielscheiben des Hasses sind Juden auch in Berlin! Die Opferberatungsstelle Reach Out *berichtet von einer gestiegenen Anzahl von rassistisch oder antisemitisch motivierten Angriffen auf jüdische Bürger in Berlin. Im Jahr 2018 wurden 309 Angriffe dokumentiert. Dies sind 46 Gewalttaten und massive Bedrohungen mehr als 2017[1]. Bei den Betroffenen können Traumata und Störungen eintreten, die sehr lange anhalten – auch lebenslang! In den Berichten darüber heißt es, das gesellschaftliche Klima sei in den vergangenen Jahren deutlich rauer geworden. Warum gehen erwachsene Männer aus rassistischen Gründen gewaltsam gegen Kinder und Jugendliche vor? Hier hat unsere Gesellschaft, hier hat Berlin, haben wir ein ernsthaftes Problem! Aus dem Entsetzen über diese Nachrichten, sind noch kurzfristig und spontan diese Thesen zu unserer Konferenz über Wissenschaftsverantwortung entstanden. Dabei stütze ich mich vor allen auf schon früher geführte Diskussionen mit meinen Freunden Hans-Alfred Rosenthal, Joseph Weizenbaum, Benno Müller-Hill, Inge und Samuel M. Rapoport sowie schon in meiner Kindheit im Faschismus mit Emil Fuchs.*

John Desmond Bernal, der Begründer der Wissenschaftsforschung (Science of Science) schrieb: „Glücklicherweise hat die Wissenschaft eine dritte bedeutsame Funktion. Sie ist die Hauptkraft für Veränderungen in der Gesellschaft; zunächst unbewusst in Form technischer Neuerungen, die den Weg zu ökonomischem und sozialem Wandel ebnen, und neuerdings als ganz bewusstes und direktes Motiv für gesellschaftliche Veränderungen selbst."[2]

1. Hier soll verdeutlicht werden, dass dieses, wie John Desmond Bernal hervorhebt, bewusste und direkte Motiv der Wissenschaft, zur gesellschaftlichen Veränderung beizutragen, verlangt, dass die Wissenschaft ihrem humanistischen Auftrag gerecht wird. Das aber heißt, dass sie mit ihren Ergebnissen zur Gewährleistung der Menschenrechte beiträgt, dass sie ihre Ver-

antwortung wahrnimmt: die Wahrheit ihrer Aussagen zu sichern und eine dem Leben, dem Menschen dienliche Anwendung der Wahrheit zu realisieren und somit auch darin ihre Verantwortung sieht, eine tiefe „Wahr-Nehmung" des Lebens und des Menschen zu befördern, nicht zu behindern, sodass die Natur und der Mensch in ihrer Spezifik und ihrem Wert erkannt und anerkannt werden.[3]

2. Die Wissenschaft soll der Förderung der Menschenrechte dienen. Wenn, wie der langjährige Leiter des TC9 der Internationalen Föderation für Informationsverarbeitung (IFIP): *Wechselbeziehungen zwischen Computer und Gesellschaft* und Präsident der IFIP, Klaus Brunnstein, wiederholt betonte, davon ausgegangen wird, dass es nicht nur individuelle sondern auch soziale sowie internationale Menschenrechte gibt, bedeutet dies z. B. für die Arbeit der InformatikerInnen, sich für den Datenschutz als individuelles Menschenrecht, für Persönlichkeitsentwicklung fördernde Arbeits- und Organisationsgestaltung als soziales Menschenrecht sowie sich für ein Leben in Frieden als internationales und erstes Menschenrecht einzusetzen. Wenn wir uns für die Gewährleistung der Menschenrechte einsetzen, steht die Unantastbarkeit der Würde eines jeden Menschen im Vordergrund und damit der Kampf gegen jede Form der Degradierung des Lebenden, des Menschen, gegen Rassismus und Antisemitismus.

3. J. D. Bernal erkannte, dass die Gesellschaft ihre anspruchsvollen Ziele nur mit Hilfe der Wissenschaft verwirklichen kann, die gesellschaftliche Wirksamkeit der Wissenschaft aber in hohem Maße von der Einführung und Beherrschung moderner Methoden und Techniken der Forschung und auch der Organisation und Leitung gesellschaftlicher Prozesse bestimmt ist. Für den Erkenntnisfortschritt ist die Zurückführung der komplexen Prozesse und Strukturen auf die ihnen zugrundeliegenden elementaren Prozesse und Strukturen eine entscheidende Voraussetzung. Dabei wird aber die Erkenntnis wichtig, dass man bei der Reduktion nicht stehen bleiben darf, denn die ist für die Erkenntnis des Ganzen zu begrenzt. Eine besondere Verantwortung der Wissenschaft ergibt sich heute insbesondere daraus, dass offensichtlich eine einseitige, reduktionistisch geprägte wissenschaftlich-technische Kultur zu einem Wahnehmungsverlust dem Leben und dem Menschen gegenüber führt. Unter bestimmten gesellschaftlichen Bedingungen kann dies wiederum von Rassisten und anderen Antihumanisten missbraucht werden.

4. Gegen Verdinglichung und Degradation des Lebenden. Das Leben ist mit seiner einzigartigen, hochkomplexen Struktur vielseitigen Gefahren ausgesetzt[4] und dies, wie viele Autoren vermerken, nicht nur durch die Veränderung äußerer Bedingungen wie durch den Treibhauseffekt, sondern auch und vielleicht noch mehr durch einen Wahrnehmungsverlust einer reduktionistisch geprägten wissenschaftlich-technischen Kultur dem Lebenden und dem Menschen gegenüber.[5] Es ist nicht die Entdeckung der Kernspaltung und der DNA und nun die Entschlüsselung des Humangenoms[6] und auch nicht die Entwicklung des Computers und gegenwärtig der globalen digitalen Netze – des Internets und des Internets der Dinge –, die diese Gefahr für unsere Welt bilden. Sie liegt vielmehr in der Tatsache einer weitgehenden Verdinglichung und Degradation des Lebenden begründet, indem alles nur noch als nutzbare Ressource betrachtet und entsprechend behandelt wird. Dieser rücksichtslose Verwertungsdrang, durch den jede neue wissenschaftliche Hypothese sofort auf den Prüfstand ihrer profitablen Anwendungsmöglichkeiten gestellt wird, prägt weithin den aktuellen Zeitgeist.

5. Es ist ein legitimes Ziel der bio-medizinischen Forschung, die Ursachen heute noch unheilbarer Krankheiten, wie Alzheimer, Krebs und Parkinson aufzudecken und nach Möglichkeiten der Heilung zu suchen. Ein Eingriff in dieses komplexe Geschehen der Lebensprozesse sollte nicht als Hybris verteufelt werden. Als Menschenrechtsverletzung entschieden abzulehnen sind jedoch die von falsch geleitetem Ehrgeiz von Wissenschaftlern entwickelten Pläne zur Verbesserung der Menschheit als Ganzem oder die von Profitgier einiger Unternehmen getriebene überstürzte Einführung von neuen Produkten. Hier tritt in der Tat die Verachtung des Menschen, die Herabwürdigung alles Lebendigen unter den herrschenden ökonomischen Kräften verabsolutierten Verwertungszwangs hervor.

6. Gegen die Reduktion des Menschen auf das Tier und den Computer. Es liegt in der Verantwortung der Wissenschaft und der WissenschaftlerInnen, dass nicht wichtige wissenschaftlich-technische Entwicklungen, zurzeit vor allem in der Informatik und in der Biologie, dazu missbraucht werden, den Menschen in seiner Komplexität, Empfindlichkeit, Einzigartigkeit, Individualität usw. zu unterschätzen oder überhaupt zu missachten. Es ist die mit den großen Erfolgen in der modernen Wissenschaft, speziell der Biologie und Informatik, verbreiteten philosophisch-weltanschaulichen Grundhaltung eines reduktiven, primitiven, mechanistischen Materialismus, der religiös fundamentalistischen Bewegungen den Nährboden liefert. Wenn generell der Geist geleugnet wird, er mit Informationsverarbeitung identifiziert und diese auf Signalverarbeitung bzw. syntaktische Informationsverarbeitung reduziert wird, wenn im Namen der modernen Wissenschaft allgemein erklärt werden kann, dass Mensch und Computer identisch sind, es sich nur um Hard- oder Feuchtware handelt, wenn als neueste Erkenntnis der Wissenschaft die Identität von Geist und Gehirn die Reduzierung des Geistes auf neuronale Verknüpfungen[7] oder Verknüpfungen kleiner Roboter[8] allerorts verkündet wird, darf man sich nicht wundern, dass bei einer weitverbreiteten Perspektivlosigkeit der Menschen damit eine Gegenreaktion ausgelöst wird, so dass, wie es selbst in den reichen Ländern zutage tritt, man sich den „intelligenten Designer" herbeiwünscht. Dass dies zu einer Massenbewegung selbst in Teilen Europas wird oder man sich anderen fundamentalistischen Gruppen und Ideengut zuwendet, durch die auch der Rassismus befördert wird. Die Reduktion von Menschen auf das Tier, die damit behauptete Minderwertigkeit in biologischer und geistiger Hinsicht von Teilen der Menschheit, war eine der wichtigen ideologischen Voraussetzungen für beide Weltkriege. Die Reduktion des Menschen auf die Maschine, das gegenwärtig verbreitete Postulat, Automaten könnten sogar bessere Menschen werden und es könnte ein postbiologisches Zeitalter anbrechen, die menschliche Gesellschaft durch eine Automatengesellschaft abgelöst werden, wie dies von dem Roboterentwickler im MIT Hans Moravec in seinem Buch *Mind Children*[9] postuliert wurde, kann die völlige Zerstörung der Menschheit vorbereiten. Auch solche falschen Ideen haben Macht, wie J. Weizenbaum[10,11] und B. Müller-Hill[12] nicht müde wurden, uns immer wieder in Erinnerung zu rufen. Sie leisten der Degradierung des Menschen und damit Rassismus und Antisemitismus Vorschub.

7. Informationsentstehung ist eine essentielle Kategorie für die Modell- und Theorienbildung in verschiedenen Grenzbereichen. Dem Reduktionismus in der Wissenschaft als einer weltanschaulichen Haltung kann und muss man entgegenwirken, indem man die Spezifik des Lebenden, speziell des Lebenden gegenüber dem Toten, speziell des Menschen gegenüber dem technischen Automaten, dem sogenannten autonomen Roboter, herausarbeitet. J. Weizenbaum stellt an Hans Morales die Frage, ob er wirklich annehmen kann, das wirklich Menschliche, z. B. ein Lächeln einer jungen Mutter zu ihrem Kind, auf die Roboter übertragen zu können.[13] […]

8. Das Konzept der Informationsentstehung – der Kreativität – erweist sich als ein allgemeiner methodologischer Leitgedanke! Die wissenschaftstheoretischen und methodologischen Implikationen des Konzepts der Kreativität – der Informationsentstehung – hat für fast alle Bereiche wissenschaftlichen Interesses an Bedeutung gewonnen. Insbesondere gibt es methodologische Hinweise zur sichereren Navigation zwischen der Scylla eines groben Reduktionismus (inspiriert durch die Physik des 19. Jahrhunderts) und im 20. Jahrhundert durch die *Geist-Gehirn-Identität* (Neurophilosophy) der konnektionistischen KI-Forschung, und der Charybdis des Dualismus (inspiriert durch den Vitalismus der Romantik des 19. Jahrhunderts und im 20. Jahrhundert durch die funktionalistische Körper-Geist / Hardware-Software-Dualität der kognitivistischen KI-Forschung. Grundlage für posthumanistische und andere antihumanistische Konzeptionen ist die Reduktion des Menschen auf ein Informationssystem und die Reduktion der Information auf ihre syntaktische Struktur, entsprechend dem Informationsverarbeitungsansatz der klassischen KI-Forschung. Der Leitgedanke der Kreativität, der Informationsentstehung im Lebenden, im schöpferischen Denken und in einer sich entwickelnden, lebendigen sozialen Organisation, führt zu einem Verständnis der Mensch-Computer-Interaktion als Koppelung maschineller (syntaktischer) Informationsverarbeitung mit dem zur semantischen Informationsverarbeitung befähigten, schöpferisch tätigen Menschen. Damit ist nicht die Superautomation, die vollständige Ersetzung des Menschen, das Ziel der Automation, sondern die sinnvolle Koppelung der jeweils spezifischen Fähigkeiten von Computer und Mensch. Damit verlieren auch die antihumanen Vorstellungen ihren theoretischen wie praktischen Boden.

9. Eine tiefere *Wahr-Nehmung* des Lebens und des Menschen ist auch in der Wirtschaft erforderlich! Eine wirklich tiefe, gegenüber der heutigen Situation vertiefte bzw. neue, *Wahr-Nehmung* des Lebenden und des Menschen wird auch in der Wirtschaft dringend gebraucht, weil gerade sie, unter dem Druck der Globalisierung und Digitalisierung, noch stärker zur Innovation gezwungen ist, neue Produkte und Dienstleistungen auf den internationalen Markt zu bringen. Dies verlangt nach immer weiterer Forschung und neuem Wissen. Es muss also nach der Verwendbarkeit des Wissens gefragt werden. Dies muss aber nicht mit einer Degradierung und Verdinglichung des Menschen und allem Lebenden verbunden sein, wie dies z. B. durch die von vielen fast unbemerkte und gerade daher weit verbreitete Identifizierung von Automat und Mensch erfolgt. Dies u. a. mit einer Wiederbelebung der Diskussion über die Möglichkeit einer Super- bzw. Vollautomatisierung im Zusammenhang mit der Entwicklung der Industrie 4.0. Die damit verbundene Herabwürdigung des Menschen nicht nur auf das Tier wie durch den Rassismus, sondern darüber hinaus auf die Maschine, kann verheerende Folgen haben. Automaten (Roboter) können Tätigkeiten des Menschen – ganze Produktionsabschnitte z. B. in der Autoindustrie – vollständig übernehmen. Eine vollständige Eliminierung des Menschen aus den Produktionsprozessen (eine menschenleere Fabrik) hält heute jedoch kaum noch jemand für wirklich erstrebenswert und möglich. Die neuen Möglichkeiten der Automation, über das Internet der Dinge (*Cyberphysical Systems*) und mit Unterstützung lernender Roboter, verlangen und ermöglichen eine sinnvolle Kombination von Automat und Mensch.

10. Zur Notwendigkeit der Erziehung und Bildung gegen Rassismus: Der Kampf gegen Rassismus muss ein wichtiges Anliegen in der Diskussion um die Verantwortung der Wissenschaft und der WissenschaftlerInnen sein. Es wurde argumentiert, dass es keiner wissenschaftlichen Argumente gegen Rassismus bedarf, da ein Humanist von vornherein gegen jede Form des Rassismus sein müsse, unabhängig von irgendeiner naturwissenschaftlichen Beweisführung. Auch wenn dies im Prinzip richtig ist, denn ethische Werte kommen nicht aus den Naturwissenschaften, sondern aus Erfahrungen des gesellschaftlichen Lebens der Menschen, so kann doch z. B. die naturwissenschaftliche Erkenntnis nützlich sein, dass es kein „Kulturgen" gibt, wie unter der Annahme eines strengen genetischen Determinismus von einigen Molekularbiologen und Philosophen postuliert wurde. Die Gene haben mit dem, was unter Mensch-Sein zu verstehen ist, nichts zu tun.[14] […]

11. Information soll nicht verdinglicht, der Mensch nicht auf seine Gene und auf den Computer reduziert werden! […]

12. Im Zeitalter der Information und des Computers muss auch die Stellung des Menschen in der Welt der Artefakte geklärt werden,[15] denn die weit verbreitete Identifikation des Menschen mit dem Computer kann in der Tat eine ähnliche enthumanisierende Funktion haben, wie die Reduktion des Menschen auf das Tier nachweislich hatte und hat. Daher ist es nicht nur von entscheidendem praktischen Wert für die Informationssystemgestaltung und Softwareentwicklung, klar zwischen maschineller (syntaktischer) und menschlicher (semantischer) Informationsverarbeitung zu unterscheiden, sondern zugleich auch von ethischem Wert, wenn die Spezifik menschlicher gegenüber maschineller Informationsverarbeitung verdeutlicht und damit ein humanistisches Menschenbild entwickelt wird. Das bedeutet in der Tat, Information darf nicht substantialisiert / naturalisiert bzw. verdinglicht werden! Die menschliche (semantische) Informationsverarbeitung darf nicht mit der maschinellen (syntaktischen) identifiziert werden, denn dies ist die Reduktion des Menschen auf die Maschine. Gerade deshalb sind die biologischen Wissenschaften sowie die Kognitionswissenschaften heute, weil die Zusammenhänge nicht bis in alle Einzel- und Feinheiten aufgeklärt sind, ein Ausgangspunkt für Sorgen und Ängste. Aber auch dann, wenn wir eines Tages alles verstehen sollten und beherrschen würden, könnten die Sorgen und Ängste noch größer geworden sein – wegen der vollständigen biologischen Manipulierbarkeit und weitgehenden technischen Rekonstruierbarkeit und Ersetzbarkeit gerade auch des Menschen. Gerade deshalb muss die ethische Diskussion mit Entschiedenheit geführt, die Frage nach der Verantwortung der Wissenschaft so nachdrücklich gestellt werden.

13. Zur Verantwortung der Wissenschaft im Kampf gegen Antisemitismus im Gedenken an die 6 Millionen europäischen Juden, die in den Konzentrations- und Vernichtungslagern des deutschen Faschismus umgebracht wurden, sollte es eine der vorrangigsten Aufgaben der Wissenschaft, speziell auch der deutschen WissenschaftlerInnen, sein, den Antisemitismus in all seinen Formen zu bekämpfen, zu einer Erziehung gegen Hass und Gewalt und Antisemitismus beizutragen und vor allen auch daran mitzuwirken, dass die gesellschaftlichen Ursachen, die eine so menschenverachtende Ideologie immer wieder hervorbringen, überwunden werden. […]

14. Tödliche Wissenschaft – Ausgrenzung von Juden, Sinti und Roma sowie Geisteskranken und Homosexuellen. Eine ganze Reihe deutscher Forscher waren tief in die Verbrechen der deutschen Faschisten verstrickt, haben sie durch ihre wissenschaftlichen Arbeiten direkt oder indirekt befördert.[16] In seinem Buch: *Die Philosophen und das Lebendige* berichtet der Kölner Molekularbiologe Benno Müller-Hill im letzten Kapitel, das überschrieben ist: „Von der Tier- und Blutmythologie zum Vernichtungskult in Auschwitz" über die „geistige Vorbereitung, die geistige Beihilfe bei der Durchführung und schließlich das Verwischen der Spuren des größten Verbrechens das je in Deutschland begangen wurde: des Aufbaus von Auschwitz als Vernichtungs- und Produktionsstätte."[17] […]

15. Die Forderung nach der Vernichtung lebensunwerten Lebens wurde „wissenschaftlich" begründet. Man fragt sich immer wieder, wie solche Grausamkeiten, Unmenschlichkeiten, wie die Aussonderung, Ausmerzung von Juden, Sinti und Roma sowie Geisteskranken geschehen konnte. Vielfach neigte man dazu, Hitler die alleinige Schuld an den großen Verbrechen zu geben. Sicher war Hitler ein besonders grausamer, brutaler Mensch. An seiner Schuld kann und soll kein Abstrich vorgenommen werden. Aber er hatte eben sehr viele, zu viele willige Helfer. Und gerade, wenn wir den Blick auf verschiedene Wissenschaftler werfen, sehen wir deutlich Wegbereiter in der Wissenschaft.[18] […] Wenn man den Blick nicht auch auf die Wissenschaftler richtet, fehlt ein wesentliches Stück zur Beantwortung der immer wieder gestellten Frage: Wie konnte das geschehen?

16. […]

17. Religiöse Überlieferungen als eine Ursache des Antisemitismus? Der evangelische Theologe Emil Fuchs schrieb schon 1920 einen entschiedenen Artikel gegen den Antisemitismus.[19] Er setzte seinen Einsatz für die Juden auch während der Zeit des Faschismus, in seiner Auslegung des Neuen Testaments, die als illegale Schriften an seine Quäkerfreunde und Vertreter des verbotenen Bundes der religiösen Sozialisten verschickt wurde, fort.[20] Er wendet sich gegen die Fehlinterpretation von Paulus, durch die Christentum und Judentum einander entgegengestellt werden und die somit den Boden für den Holocaust bereitet hat. […] Mit erstaunlicher Hellsicht entwickelt Fuchs ein neues Paradigma der Paulusauslegung in Antithese sowohl zum herrschenden Antisemitismus wie auch Staatskonservatismus der kirchlich und universitär etablierten Theologie, hebt die Theologin Brigitte Kahl hervor.[21]

18. Zu Ursachen für Antihumanismus, Rassismus, Antisemitismus und Neo-Nazismus in der gegenwärtigen Arbeitswelt. Wir erleben gegenwärtig eine Erstarkung nazistischen, d. h. neofaschistischen Denkens in der Gesellschaft, speziell auch in den Betrieben, die ganz offensichtlich ihren Nährboden in der gegenwärtigen Arbeitswelt haben. In einer Vielzahl von Veröffentlichungen dazu wird von Erfolgen des Rechtspopulismus gesprochen, die „zum Teil überdurchschnittlich" auch unter Gewerkschaftsmitgliedern erzielt wurden.[22] Wie im heutigen politischen Sprachgebrauch praktiziert, wird, wahrscheinlich in der Hoffnung, die braun infizierten Menschen zurückzugewinnen, sie daher nicht vorschnell abzustempeln, von Rechtpopulismus gesprochen. Dies mag aus dieser Sicht richtig sein, für mich ist es eine Verharmlosung. Das, was uns heute in ganz Europa und in den USA als ein deutlicher Rechtsruck und damit verbundenem antihumanistischem Denken entgegentritt, verfolgt das schon von den deutschen Faschisten erfolgreich praktizierte Schema: Es werden reale Missstände aufgegriffen und offen kritisiert, ohne jedoch zu deren Bewältigung eine Lösung zu haben. Daher wird dann ein Schuldiger gesucht. Damals waren es die Juden. Heute sind es die Ausländer und eben schrittweise, nicht nur in Deutschland, auch wieder die Juden. […]

19. Die Arbeitenden haben ein Recht auf wissenschaftlich begründete Aussagen über die realen Verhältnisse in der Welt der Arbeit. Sie haben ein Recht darauf, dass die Arbeitswelt human gestaltet wird. Damit sind insbesondere die InformatikerInnen, die Arbeitswissenschaftler und Organisationsentwickler angesprochen. Eine am Menschen orientierte Einführung der modernen Informations- und Kommunikationstechnologien verlangt eine soziotechnische Gestaltung der Arbeitswelt, eine Informationssystem-, Arbeits- und Organisationsgestaltung aus ganzheitlicher Sicht. Dies ist eine große wissenschaftliche Herausforderung, die weder theoretisch, methodologisch noch praktisch einfach zu bewältigen ist. Deren Bewältigung große Anstrengung, beginnend mit der Ausbildung auf den Wissenschaftsgebieten, die unmittelbar mit der Gestaltung der Arbeitswelt beschäftigt sind, erforderlich macht. Unter der Decke einer viel gelobten Erfolgsökonomie haben sich die Verhältnisse in der Arbeitswelt zugespitzt. Dies führt zur Erstarkung der extremen Rechten und damit, verbunden mit der Radikalisierung des Rassismus, eines Antisemitismus, der zu offenen Attacken gegen Menschen führt, die sich durch das Tragen der Kippa als Juden zu erkennen geben. Der Antisemitismusbeauftragte der Bundesregierung rät schon dazu, an bestimmten Orten sich nicht mehr in dieser Weise zu zeigen. Der Zusammenhang zwischen der Zuspitzung der betrieblichen Arbeitsbedingungen und dieser Verstärkung des Antihumanismus, der Erhöhung der Brutalität gegen Ausländer und Juden besteht nicht nur unmittelbar, sondern hat oftmals eine Vielzahl von Vermittlungen. Neben unmittelbaren und realen Ängsten vor dem Verlust des Arbeitsplatzes kommen subjektiv verarbeitete Ängste aus den betrieblichen Arbeitsbedingungen, Abwertungserfahrungen und vieles mehr.

20. Die Angst vor dem Verlust des Arbeitsplatzes durch strukturelle Veränderungen in der Industrie und im Dienstleistungsbereich ist real, z. B. mit der angestrebten Umstellung von Diesel- und Benzinmotoren auf Elektromotoren sowie mit weiteren Mobilitätskonzepten. Die Leitung von VW sagt deutlich, dass für den Bau des Elektroautos weniger Arbeitskräfte benötigt werden. Gleichzeitig wird verkündet, dass VW mit Amazon in Verbindung steht, damit Amazon ein Konzept zur elektro-

nischen Steuerung von Produktionsprozessen in allen Werken entwickelt und einführt. Womit wiederum eine Vielzahl von Arbeitsplätzen, diesmal vor allem auch in der Verwaltung, verloren gingen. Die Durchführung und Ankündigung von Maßnahmen ständiger Umstrukturierungen in den Betrieben sind in der Tat eine reale Quelle für Verunsicherung und Ängste. Dies nicht nur in der Autoindustrie, sondern Personalabbau und damit erhöhter Leistungsdruck wird auch bei den Banken und Sparkassen erlebt und selbst in dem expandierenden Logistik- und Telekommunikationsbereich. Diese Strukturveränderungen sind meist mit der Digitalisierung und dem Einsatz der modernen Informations- und Kommunikationstechnologien (IKT) verbunden. Dieser Einsatz hat aber unabhängig davon, dass diese allgemeinen Strukturveränderungen von dem IKT-Einsatz katalysiert werden, auch weitergehende Wirkungen auf die Arbeitsverhältnisse, die Qualifikationsanforderungen und insbesondere auf andere und erhöhte Leistungskontrollen. Es gehört zur Verantwortung der Wissenschaft, dafür Sorge zu tragen, dass der Einsatz dieser Methoden und Technologien nicht allein technikorientiert, sondern vorrangig am Menschen orientiert erfolgt.[23]

21. Wo auch immer die Gründe dafür liegen mögen, dass die Thematik *Humanisierung der Arbeit* bzw. *Arbeitsgestaltung* im Rahmen der Informatik und auch im Rahmen der Teildisziplin *Informatik und Gesellschaft* aufgegeben wurde, es entsprach auf jeden Fall dem Geist der Zeit. Es ist ein Beispiel, wie es gelingt, dass sich selbst das Denken des Mainstreams an Universitäten durchsetzen kann. „Auch der wissenschaftliche Mainstream folgt mitunter der Meinung der Mächtigen."[24] Wohin diese Verabschiedung bzw. diese Abwendung der Wissenschaft bzw. der WissenschaftlerInnen, einschließlich auch der InformatikerInnen geführt hat, schildert der bekannte Philosoph Axel Honneth sehr plastisch. Er schreibt in einem Artikel in der *Deutschen Zeitschrift für Philosophie* zur bisherigen Entwicklung: „Noch nie in den letzten zweihundert Jahren hat es um Bemühungen, einen emanzipatorischen, humanen Begriff der Arbeit zu verteidigen, so schlecht gestanden wie heute. Die faktische Entwicklung in der Organisation von Industrie- und Dienstleistungsarbeit scheint allen Versuchen, die Qualität der Arbeit zu verbessern, den Boden entzogen zu haben …" Er schreibt weiter: „Was sich in der faktischen Organisation der Arbeit vollzieht, die Tendenz zur Rückkehr einer sozial ungeschützten Leih-, Teil- und Heimarbeit, spiegelt sich in verquerter Weise auch in der Verschiebung von intellektuellen Aufmerksamkeiten und gesellschaftlichen Interessen: Enttäuscht haben diejenigen, die noch vor vierzig Jahren alle Hoffnung auf die Humanisierung oder Emanzipierung der Arbeit setzten, der Arbeitswelt den Rücken gekehrt, um sich ganz anderen, produktionsfernen Themen zuzuwenden."[25] Das Interessante ist: erstens sagt Honneth, die Arbeitssituation habe sich vielfach verschlechtert. Sie kennen ja die ganze Diskussion um den Mindestlohn, die jetzt geführt wurde. In jüngster Zeit ist wenigstens da etwas korrigiert worden. Es hat sich aber auch noch etwas anderes verschlechtert. Wie Honneth sagt, ist die Zuwendung derjenigen, die sich mit den Problemen der Arbeit früher stark beschäftigten, wesentlich geringer geworden. Vor etwa 40 Jahren hat Willy Brandt als Bundeskanzler eine ganze Bewegung entfaltet, die das Ziel hatte, die Qualität des Arbeitslebens zu verbessern. Da waren auch viele Forschungsthemen darauf ausgerichtet. Wenn wir heute fragen, ist kaum noch etwas darauf ausgerichtet, selbst in der Informatik[26].

22. Die Sozialwissenschaften und die Informatik haben sich also eher von der Thematik *Zukunft und Gestaltung* der Arbeit entfernt, in der Informatik wurden beispielsweise in den letzten Jahren fast alle Lehrstühle, die das Thema *Informatik und Gesellschaft* behandelten, geschlossen.[27] Dafür wurde das Wissenschaftsgebiet *Informatik und Gesellschaft* durch die Einrichtung neuer Forschungsinstitute zur Thematik: *Ethik in der Künstlichen Intelligenz*, gefördert durch Facebook, an der Technischen Universität München und zur Thematik: *Internet und Gesellschaft*, finanziert durch Google, an der Humboldt-Universität zu Berlin, fortgeführt. Diese Entwicklung unterstreicht die Dringlichkeit und Bedeutung der zu behandelnden Themen, kann unter Umständen aber auch die Unabhängigkeit der Forschung von äußeren Einflüssen gefährden. Genau so, wie Chr. Felber es schildert, wie z. B. durch Stiftungsprofessuren oder auch durch große Konzerne finanzierte Institute oder schon über die Drittmittelforschung das Mainstreamdenken durchgesetzt wird, erfolgten nun auch auf dem Gebiet *Informatik und Gesellschaft* entsprechende Gründungen an verschiedenen Universitäten. Dies zeigt deutlich, dass die Wissenschaft nicht geschützt ist vor außerwissenschaftlicher Einflussnahme. Die Gewährleistung humanistischen Denkens ist daher eine gesamtgesellschaftliche Aufgabe. Es gilt, alle Kräfte gegen jede Form des Antihumanismus zu mobilisieren! Dazu gehört auch die Ablehnung der Verantwortung für eine humane Gestaltung der Arbeitswelt. Erfreulicherweise sind nun, ins besonders mit der Schrittweisen Realisierung der Vision der Entwicklung der Industrie 4.0, die wissenschaftlichen Aktivitäten die sich mit der Gestaltung der Arbeitswelt beschäftigen wieder wesentlich angestiegen. So gibt es jetzt eine ganze Reihe neuer soziologischer und arbeitswissenschaftlicher Studien und philosophischer Arbeiten zum Thema: *Zukunft der Arbeit*.[28,29,30,31,32] Das Ringen gegen jede Form des Antihumanismus, speziell gegen Rassismus und Antisemitismus sollte von der Erkenntnis getragen sein, dass, wer den Antihumanismus wirklich überwinden will, die Ordnung ändern muss, die ihn immer wieder gebiert. Auch eine redliche Bemühung um humanitäre Gesinnung, um soziale Gerechtigkeit und Frieden ist letztlich nicht konsequent genug, wenn sie nicht auch nach den letzten sozialen Ursachen fragt, den Ungerechtigkeiten der Gesellschaft, die sich aus den bestehenden Ausbeutungsverhältnissen, der immer größer werdenden Spaltung in Arm und Reich ergeben.

23. Die Menschen müssen Sinn und Ziel ihrer Existenz erkennen können. […]

24. Der Irrationalismus, auch in der Form des Antisemitismus, kann nur überwunden werden, wenn den Menschen Sinn und Ziel ihrer Existenz deutlich gemacht wird. Nur wo Menschen ein Ziel haben, es auch für die Entwicklung der Gesellschaft eine Perspektive gibt, werden ihre schöpferischen Kräfte geweckt. […]

25. Es gilt den Frieden zu sichern! Die meisten Menschen wollen Frieden. Ein Leben in Frieden ist das erste Menschenrecht! Sie sind sich also im anzustrebenden Ziel einig. Die Unterschiede im konkreten Wollen beziehen sich nicht auf das Ziel des Wollens, sondern auf den Weg, mit dem das Ziel erreicht werden soll. Der Frieden sei durch Aufrüstung und Abschreckung zu wahren, oder durch Verhandlungen und Bündnispolitik – welcher Weg der beste ist, um den Frieden zu erhalten, sagt uns die

Erkenntnis der Situation. Es ist sehr wichtig, festzustellen, dass hier eine Sachfrage vorliegt, die nicht durch ein logisches Modell entschieden werden kann. Wie der Positivismus verdeutlicht hat, sind logische Aussagen nur deshalb wahr, weil sie leer sind, nichts über die Wirklichkeit aussagen. Ihre Wahrheit beruht auf der Stimmigkeit des Systems. Herrscht ein Imperialismus der instrumentellen Vernunft (Max Horkheimer, Josef Weizenbaum), die Dominanz einer technisch-rationalen Vernunft, die sich mit gesellschaftlicher Herrschaft verbindet, können große Irrtümer erzeugt werden. Denn man verlässt sich auf mathematische Berechnungen, da, wo es um sachgerechte Beurteilung der gesellschaftlichen Situation gehen muss. Besonders wichtige, insbesondere menschliche Faktoren werden oder können gar nicht in die Modellrechnung mit aufgenommen werden. „Es fehlen außerordentlich wichtige Worte in dem Alltagsvokabular der Moderne. Es fehlen eben entscheidend kritische Gedanken, Ideen, die mit Menschen, mit dem Leben in der aktuellen Praxis der alltäglichen Angelegenheiten unserer Welt zu tun haben", warnt Weizenbaum.[33]

26. Die Drohung der Kündigung des INF-Vertrags zwischen den USA und Russland zeigt, wie schnell sich die militärische Konfrontation wieder zuspitzen kann. Mit diesem Abkommen wurde es Ende der 80-er Jahre möglich, atomare Kurz- und Mittelstreckenraketen abzurüsten und zu verbieten. Nun hat sich die politische Lage wieder verschärft. Selbst in Deutschland wird die Entwicklung eigener Atomwaffen diskutiert. Man spricht schon von einem neuen *Kalten Krieg*! […]

27. Es liegt entscheidend mit in der Verantwortung der Wissenschaft und der Wissenschaftler, sich gegen eine solche Entwicklung zu wenden und die Menschen dagegen zu mobilisieren. Es darf nie wieder einen Weltkrieg geben! Einen Krieg, in dem die furchtbaren Waffen, die auf Kernspaltung und Kernfusion, die auf Raketentechnik oder Informations- und Kommunikationstechnologien beruhen, eingesetzt werden. Daraus erwächst die Verantwortung und außerordentlich große Herausforderung an die gegenwärtige Wissenschaft, insbesondere an die PhysikerInnen, ein effektives Kontrollsystem zur Abschaffung der Waffen aufzubauen (vgl. *Appell aus Berlin*[34]). Jedoch berichten die Zeitungen in diesen Tagen, dass das Wettrüsten schon in Gang ist. Es wird eine neue Raketenabwehr durch Hyperschall-Waffen angekündigt. „Sowohl bei den Mittelstreckenraketen als auch bei den Hyperschallraketen ist die Vorwarnzeit so kurz, dass eine seriöse Klärung der Lage aus militärischer Sicht nicht mehr möglich erscheint. Es bleibt schlicht keine Zeit, festzustellen, ob ein Angriff begonnen hat – oder ob es auf der gegnerischen Seite vielleicht nur eine Panne gibt. Ein Krieg aus Versehen zählt zu den Horrorvisionen bei allen Militärs", schreiben Marina Kormbaki und Stefan Koch in der Berliner Zeitung aus Washington.[35] Die Situation hat sich offensichtlich gegenüber der, in der sich der Informatiker David Parnas aus persönlicher Verantwortung der von Ronald Reagan in einer angespannten Phase des Kalten Krieges, initiierten *Strategic Defense Initiative* verweigerte, in der sich die Informatiker Klaus Brunnstein, Wilhelm Steinmüller, Klaus Haefner u. a. an das Bundesverfassungsgericht wandten, da der Bundespräsident in einer solchen Situation den Schutz der Bevölkerung nicht mehr sichern kann, noch wesentlich verschärft. Daher sollten wir diese Tradition nicht vergessen, sondern fortführen. […]

28. Es hat immer wieder Versuche gegeben, zu erklären, wie dieser Sturz in den Abgrund geschehen konnte. Auch wenn viele Fragen dazu geklärt werden konnten, blieben doch sehr viele Fragen offen. Es gibt wahrscheinlich keine erschöpfende Antwort auf die Frage, wie aus dem Land der Dichter und Denker eines des Völkermordes werden konnte. […]

29. Die Menschheit muss lernen, sich als ein Ganzes zu verstehen und zu organisieren. Dies hat aber zur Voraussetzung, dass die Menschheit lernt, ihren Stoffwechsel mit der Natur gemeinsam zu gestalten. […]

30. Eine mögliche Krise der Wissenschaft kann, wie J. Mittelstraß aufgezeigt hat, durch die drohende Distanz zwischen Erzeugung und Nutzung des Wissens entstehen, wodurch der Wissensprozess beschädigt wird, indem das Wissen sein eigentliches Wesen verliert, „nämlich Ausdruck des epistemischen Wesens des Menschen zu sein".[36] Wenn wir von der Verantwortung der Wissenschaft für die Gewährleistung der Menschenrechte – Im Kampf gegen die Degradation des Lebenden, Rassismus und Antisemitismus sprechen und aufgezeigt haben, dass die Wissenschaft selbst, durch verfehlte Schlussfolgerungen, durch ein Stehenbleiben bei der methodologisch erforderlichen Reduktion oder dem Nachgeben gegenüber überhöhtem Verwertungszwang, mit der „drohenden Distanz zwischen Erzeugung und Nutzung des Wissens" zumindest zum Katalysator sich in der Gesellschaft herausgebildeter menschenfeindlicher Ideologien werden kann, so ist doch festzuhalten, dass die Wissenschaft methodisch gesichertes Wissen gewinnen will. […]

31. Von allen möglichen Formen menschlicher Erkenntnis ist es die Wissenschaft, die sich grundsätzlich bemüht, methodisch gesicherte Erkenntnisse zu gewinnen. Sie wehrt sich daher zu Recht gegen außerwissenschaftliche Beeinflussung. Sie wendet sich daher auch dagegen, wenn Forschungsvorhaben durch nicht rational begründete Werturteile behindert werden. Das kann aber nicht heißen, dass eine positivistische Position eingenommen und jede ethische Beurteilung wissenschaftlicher Tätigkeit abgelehnt wird. […]

32. Wissenschaftler erheben gerne die „Objektivität" zum alleinigen, höchsten Wert der Wissenschaft und lehnen eine weitere Wertung ab. Damit erscheint alles als machbar. Aus der erschütternden Erfahrung, dass dies den Weg zu einer tödlichen Wissenschaft geebnet hat, müssen wir aber lernen, dass es nicht erlaubt ist, alles zu machen, was man machen kann. […]

33. […]

34. Es bedarf einer Vertiefung des humanistischen Denkens, ausgehend von einer umfassenderen Bestimmung des Wesens des Menschen. Auf dieser Grundlage geht es um die Gewinnung einer neuen Haltung zum Seienden und Werdenden, bei der die Dinge nicht mehr allein als die vermittels der wissenschaftlichen Erkenntnis zu beherrschenden Objekte gesehen werden. Erkenntnis muss als Teilhabe an Natur und Gesellschaft verstanden werden. Verlangt wird eine Haltung, die von der Achtung gegenüber den Naturwesen, der Teilnahme an ihrem Dasein ausgeht, die den Menschen als Teil der Natur sowie vorrangig soziales und gesellschaftliches Wesen versteht, die Würde jedes Menschen respektiert. Der Mensch ist das ein-

zige Lebewesen, welches sich in der menschlichen Gesellschaft zu einer Persönlichkeit entwickelt und sich seines Menschseins – Mensch unter Menschen zu sein – immer stärker bewusst werden kann.

Nachtrag: Die Verbrechen der Vergangenheit dürfen nicht vergessen werden. Daher stellte sich auch die Max-Planck-Gesellschaft zu ihrem 100-jährigen Bestehen den dunklen Ereignissen in ihrer Vergangenheit. Sie hatte 30 Jahre nach der Befreiung vom Faschismus damit begonnen. Natürlich zu spät! Aber, es ist nie zu spät, die wichtigste moralische Verpflichtung für uns heute zu erkennen, die darin besteht, für eine vollständige Aufklärung eben auch der Verbrechen von Wissenschaftlern zu sorgen und sich dafür einzusetzen, dass eine Wiederholung völlig ausgeschlossen wird. Die für diese Konferenz zur Wissenschaftsverantwortung vorgelegten Thesen sind kurzfristig, als spontane Reaktion auf dem großen Schreck über diese Geschehnisse in Berlin wie auch in anderen Gegenden Deutschlands und der Welt entstanden. Sie sind daher keine systematische Darstellung des gegenwärtigen Antisemitismusproblems. Es galt, die Verantwortung der Wissenschaft für geschehenes Unrecht und für die Wahrnehmung ihres humanistischen Auftrages aufzuzeigen. Daher wurde die Thesenform für meinen Beitrag beibehalten Zur Entwicklung des Rassismus und Antisemitismus heute liegt umfangreiche Literatur vor. Hier sei nur auf drei jüngere Arbeiten, wie auch schon im Text, verwiesen.[37,38,39,40,41] In diesen Arbeiten wird auf die vielfältigen ökonomischen und sozialen Ursachen für den heutigen Antisemitismus eingegangen. In der Diskussion dieser Thesen mit Victor G. Mairanowski, für die ich ihm danke, wurde mir insbesondere deutlich, wie stark diese negative Entwicklung in unserer Stadt auch von einem importierten Antisemitismus beeinflusst wird. In der Stadt leben Menschen aus 180 Nationen, die zu einem großen Teil mit Antisemitismus in ihren Heimatländern aufgewachsen sind. Wir müssen uns aber eingestehen, dass der Antisemitismus bei uns auch nie weg war. Daher sei hier speziell noch auf das, von Andreas Nachama, Julius H. Schoeps, Hermann Simon herausgegebene Buch: *Juden in Berlin*[42] verwiesen, das einen tiefen Eindruck darüber vermittelt, welche Bedeutung jüdisches Leben in unserer Stadt, für diese Stadt hatte und welche Konflikte es dabei von Beginn an gab. Auf diesem Hintergrund, der praktischen Vernichtung allen jüdischen Lebens in der Stadt durch den deutschen Faschismus, gewinnt das Buch von Victor G. Mairanowski: *20 Jahre Einzigartige Aktivitäten – Eingewanderte jüdische Wissenschaftler in Berlin*,[43] in dem von dem schwierigen aber erfolgreichen Neuanfang jüdischer Einwanderer aus der ehemaligen Sowjetunion berichtet wird, besonderes Gewicht.

Es sei hier noch auf zwei weitere wichtige Veröffentlichungen der jüngsten Zeit verwiesen, die uns sehr klar die Gefahr des gegenwärtigen Rechtsrucks und die Gründe dafür vor Augen führen. Einmal das Buch von Daniela Dahn: „Der Schnee von Gestern ist die Sintflut von Morgen. – Die Einheit – Eine Abrechnung“[44] und zum anderen das Buch von Mathias Quent: „Deutsch Land Rechts Aussen“[45]. Daniela Dahn verdeutlicht, dass die „siegreiche“ Demokratie überall an Vertrauen verloren hat, weil sie von den Eliten, die sie tragen sollen, permanent entwertet wird. Daniela Dahn arbeitet heraus: „Bevor der Rechtextremismus die Mitte der Gesellschaft erreicht hat, kam er aus der Mitte des Staates.“[46] Unter der Überschrift: *Universitäten* verweist sie auf ein dafür besonders gravierendes Beispiel, die Vergabe der ersten Ehrendoktorwürde nach der Wende durch die Humboldt-Universität an den Generalstabsoffizier und Kommandeur der SS-Panzergrenadier-Division *Götz von Berlichingen*. Dies geschah, trotz der Proteste der Studenten und des genannten Professors Frank Hörnigk. Als Landesvorsitzender des Berliner Verbandes Hochschule und Wissenschaft (VHW-Berlin, Teilgewerkschaft im Berliner Beamtenbund/ Tarifunion), dem damals insbesondere Professorinnen und Professoren der Humboldt-Universität angehörten, protestierte auch ich energisch. Dies führte zu einem Briefwechsel zwischen der damaligen Präsidentin der Humboldt-Universität und mir. Es half alles nichts. Der Ehrendoktor für einen Kommandeur einer SS-Division, von der Teile noch in Prag kämpften, als in Berlin die Kämpfe schon beendet waren, deren Einheiten, wie D. Dahn noch recherchiert hat, Massaker an griechischen Zivilisten verübt hatten, blieb bestehen. Welche Macht müssen die Mächte der Vergangenheit damals schon wieder bzw. noch besessen haben, um gleich nach der Wende einen weiteren Ehrendoktor für Wilhelm Krelle durchzusetzen? Wenn man dies erlebt hat, dann wird man durch den Untertitel des Buches Mathias Quent: „Wie die Rechten nach der Macht greifen“, nicht mehr überrascht. Der Titel geht aber noch weiter „…und wie wir sie stoppen können.“ Er zeigt also auch, wie der jetzige Rechtsruck durch unser Engagement aufgehalten werden kann und unbedingt aufgehalten werden muss.

Es liegt mir jetzt auch das vom Berliner Senat beschlossene *Berliner Landeskonzept zur Weiterentwicklung der Antisemitismus-Prävention*[47] vor. Es ist erfreulich und sehr ermutigend, daraus zu ersehen, welche Kraftanstrengung die Stadt Berlin unternimmt, sich dem erneuten Ausbruch rassistischer, antisemitischer Verunglimpfungen und Gewalttätigkeiten durch umfassende präventive Maßnahmen entschieden entgegenzustellen. Hier sind eine Reihe konkreter Handlungsfelder vorgesehen: zur Bildung der Jugend und der Erwachsenen, Justiz und innere Sicherheit, Jüdisches Leben in der Berliner Stadtkultur, Antidiskriminierung, Opferschutz und Prävention, und auch Wissenschaft und Forschung wird als ein konkretes Handlungsfeld in der Berliner Konzeption zur Prävention von Antisemitismus genannt. Dass dies alles leider sehr notwendig ist, wird besonders deutlich in der Verlautbarung des Antisemitismusbeauftragten der Bundesregierung, der den Juden in Deutschland dazu geraten hat, ihre Kippa nicht überall öffentlich zu tragen. Dies wurde weithin als „Kapitulation vor dem Antisemitismus“[48] angesehen. Dies darf keinesfalls geschehen! Es muss gewährleistet werden, dass Juden sich überall in Deutschland angstfrei bewegen und zu erkennen geben können. Dazu muss die Zivilgesellschaft aufgerüttelt werden und die Verbrecher auch strafrechtlich belangt werden. Das schulden wir: „Den 6 Millionen, die keine Retter fanden.“

Quelle: Mieg HA, Lenk H Hg. (2019). Wissenschaftsverantwortung: Wissenschaftsforschung Jahrbuch 2019 (Gesellschaft für Wissenschaftsforschung). Berlin: wvb.

Diese Fassung musste aus Platzgründen gekürzt werden und wurde vom Autor nachbearbeitet und ergänzt.

Anmerkungen

1 *Leister A (2019) Zielscheibe des Hasses, Berliner Zeitung Nr. 56, 2019, S. 15*

2 *Zitiert nach Laitko H, Trunschke A Hg. (2003) Mit der Wissenschaft in die Zukunft – Nachlese zu John Desmond Bernal, Schkeuditz, Klappentext.*

3 *Alter G, Böhme G, Ott H Hg. (2000) Natur Erkennen und Anerkennen, Über ethikrelevante Wissenszugänge zur Natur, Die graue Edition, F.W. Wessel, Baden-Baden*

4 *Fischbeck HJ Hg. Leben in Gefahr?, Von der Erkenntnis des Lebens zu einer neuen Ethik des Lebendigen.*

5 *ebenda (Klappentext)*

6 *Fuchs-Kittowski K, Rosenthal HA, Rosenthal A (2005) Die Entschlüsselung des Humangenoms – ambivalente Auswirkungen auf Gesellschaft und Wissenschaft, in: Erwägen Wissen Ethik, Deliberation Knowledge Ethics, EWE 16 (2005) Heft 2 / Issue 2, S. 149-162 (Hauptartikel), Geistes- und Naturwissenschaften im Dialog 219-234 (Replik)*

7 *Crick F (1994) Was die Seele wirklich ist – Die naturwissenschaftliche Erforschung des Bewußtseins, Artemis & Winkler, München und Zürich*

8 *Dennett DC (2006) Süße Träume – Die Erforschung des Bewusstseins und der Schlaf der Philosophie, Suhrkamp, Frankfurt am Main*

9 *Moravec H (1990) Mind Children: The Future of Robot and Human Intelligence, Harvard University Press*

10 *Weizenbaum J (1976) Die Macht der Computer und die Ohnmacht der Vernunft, Suhrkamp Taschenbuch, Wissenschaft, Frankfurt am Main*

11 *Weizenbaum J (2001) Computermacht und Gesellschaft, Suhrkamp Taschenbuch, Wissenschaft, Frankfurt am Main*

12 *Müller-Hill B (1981) Die Philosophie und das Lebendige, Campus Verlag, Frankfurt/ New York*

13 *Weizenbaum J (1991) Das Menschenbild im Lichte der künstlichen Intelligenz, In: Margarete Mitcherlich et al. (Hg.): Prioritäten, Pendo Verlag, Zürich*

14 *Fuchs-Kittowki K, Fuchs-Kittowski M, Rosenthal HA (1983) Biologisches und Soziales im menschlichen Verhalten, In: Deutsche Zeitschrift für Philosophie, Heft 7, S. 812-824*

15 *Fuchs-Kittowki K (2016) Stellung und Verantwortung des Menschen in komplexen informationstechnologischen Systemen. in: Wirtschaftsinformatik & Management, Springer / Gabler, 2/2016, S. 10-21*

16 *Max-Planck-Institut – Präsident Markl entschuldigt sich bei den Opfern medizinischer Versuche während des Nationalsozialismus, https://www.mpg.de/955395/46_person8-2001*

17 *Müller-Hill B (1981): Die Philosophen und das Lebendige, Campus Verlag, Frankfurt/ New York*

18 *Müller-Hill B (1984) Tödliche Wissenschaft. Die Aussonderung von Juden, Zigeunern und Geisteskranken 1933-1945, Rowohlt; Hamburg*

19 *Fuchs E (1920) Antisemitismus, Deutsche Politik*

20 *Fuchs-Kittowski K (2016) Emil Fuchs. Christ, Sozialist und Antifaschist. Freund des arbeitenden Volkes, in: Beiträge zur Geschichte der Arbeiterbewegung, 4/2016, S. 67-165*

21 *Kahl B (2018) Emil Fuchs` Römerbriefauslegung im Kontext gegenwärtiger Pauluskontroversen, in: Banse G, Kahl B, Rehmann J Hg. (2018) Marxismus und Theologie. Materialien der Jahrestagung 2018 der Leibniz-Sozietät der Wissenschaften, Abhandlungen der Leibniz-Sozietät der Wissenschaften, Band 55, travo Wissenschaftsverlag, Berlin, 20 – 19, S. 71-80*

22 *Sauer D, Stöger U, Bischoff J, Detja R, Müller B (2018) Rechtspopulismus und Gewerkschaften – Eine arbeitsweltliche Spurensuche, VSA: Verlag Hamburg, Klappentext*

23 *Fuchs-Kittowki K (2010) Information, Organisation und Informationstechnologie – Schritte zur Herausbildung einer am Menschen orientierten Methodologie der Informationssystem- Arbeits- und Organisationsgestaltung. in: Coy W, Schirmbacher P Hg. (2010) Informatik in der DDR – Tagung Berlin, Humboldt- Universität zu Berlin, http: edoc.hu-berlin.de/conferences/iddr2010/ S. 7-36*

24 *Felber C (2018) Gemeinwohlökonomie, Piper, S. 135*

25 *Honneth A (2008) Arbeit und Anerkennung – Versuch einer Neubestimmung. In: Deutsche Zeitschrift für Philosophie (Berlin) Nr. 3, S. 327-341*

26 *Fuchs-Kittowski K (2002) Schwierigkeiten mit dem sozialen Aspekt, in: FIfF-Kommunikation. 3/2002, S. 57-58*

27 *Fuchs-Kittowski K (2013) Die Schwierigkeiten mit dem sozialen Aspekt – Zur Umprofilierung des Lehrstuhls Informatik in Bildung und Gesellschaft an der Humboldt-Universität zu Berlin, in: FIfF-Kommunikation 4/2013, S. 31-33.*

28 *Krämer J, Richter J, Wendel J, Zinssmeister G Hg. (1987) Schöne Neue Arbeit – Die Zukunft der Arbeit vor dem Hintergrund neuer Informationstechnologien, Talheimer Verlag, Mössingen-Talheim*

29 *Kornwachs K Hg. (2004) Technik – System – Verantwortung, Technikphilosophie Bd. 10, LIT- Verlag, Münster*

30 *Schröter W Hg. (2014) Identität in der Virtualität, Talheimer Verlag, Mössingen-Talheim*

31 *Botthof A, Hartmann EA Hg (2014) Zukunft der Arbeit in Industrie 4.0, Springer Vieweg, Berlin, Heidelberg*

32 *Werther S, Bruckner L Hg. (2018) Arbeit 4.0 aktiv gestalten – Zukunft der Arbeit zwischen Agilität, People Analytics und Digitalisierung, Springer-Verlag*

33 *Weizenbaum J (2002) Lecture at the Occasion of the Dagmar and Václav Havel Foundation VIZE 97 Prize October 5, 2002: Wider den Zeitgeist!*

34 *Appell aus Berlin – Für ein kontrollierbares Abkommen zur Abschaffung aller Atomwaffen. In: Flach G, Fuchs-Kittowki K Hg. (2012) Vom atomaren Patt zu einer von Atomwaffen freien Welt – Zum Gedenken an Klaus Fuchs, Abhandlungen der Leibniz-Sozietät, trafo wissenschaftsverlag, Berlin, S. 483-484*

Klaus Fuchs-Kittowski

Prof. Dr. habil. **Klaus Fuchs-Kittowski** (Jahrgang 1934) ist Professor für Informationsverarbeitung. Er war Leiter des Bereichs Systemgestaltung und automatisierte Informationsverarbeitung der Sektion Wissenschaftstheorie und Wissenschaftsorganisation der Humboldt-Universität zu Berlin. Er war Mitglied des TC 9 (Wechselbeziehungen zwischen Computer und Gesellschaft) der Internationalen Föderation für Informationsverarbeitung (IFIP) und langjähriger Chairman der WG 9.1 (Computer und Arbeit) des TC 9 der IFIP und ist Mitglied der Leibniz-Sozietät der Wissenschaften.
E-Mail: *fuchs-kittowski@t-online.de*

35 Kormbaki M, Koch S (2019), Berliner Zeitung Nr. 17, 21 Januar 2019, S. 2
36 Mittelstraß J (2001) Krise des Wissens? – Über die Erosionen des Wissens- und Forschungsbegriffs, Wissen als Ware, Information statt Wissen und drohende Forschungs- und Wissenschaftsverbote. In: Sitzungsberichte der Leibniz-Sozietät, Band 47, Heft 4, S. 21–42.
37 Salzborn S (2018) Globaler Antisemitismus – Eine Spurensuche in den Abgründen der Moderne, Beitz Juventa
38 Landeszentrale für politische Bildung Baden-Württemberg (Hg.) Der Bürger im Staat – Antisemitismus heute.
39 Rensmann L (2001) Kritische Theorie über den Antisemitismus. Studien zu Struktur, Erklärungspotential und Aktualität
40 Holz K (2005) Die Gegenwart des Antisemitismus. Islamistische, demokratische und antizionistische Judenfeindschaft.
41 Heilbronn C, Rabinovici D, Sznaider N (2019) Neuer Antisemitismus? – Fortsetzung einer globalen Debatte, Berlin: Suhrkamp-Verlag
42 Nachama A, Schoeps JH, Simon H Hg. (2001) Juden in Berlin Berlin: Henschel-Verlag
43 Mairanowski VG (2018) 20 Jahre Einzigartige Aktivitäten – Eingewanderte jüdische Wissenschaftler in Berlin, Wissenschaftliche Gesellschaft WiGB bei der jüdischen Gemeinde zu Berlin, Berlin
44 Dahn D (2019) Der Schnee von Gestern ist die Sintflut von Morgen – Die Einheit – Eine Abrechnung, Rowohlt Taschenbuch Verlag, Hamburg
45 Quent M (2019) Deutsch Land Rechts Aussen – Wie die Rechten nach der Macht greifen und wie wir sie stoppen können, Piper-Verlag, München
46 Dahn D (2019) a.a.O., Klappentext
47 Berlin gegen jeden Antisemitismus! Berliner Landeskonzept zur Weiterentwicklung der Antisemitismus-Prävention.
48 Berliner Zeitung (2019) 121/2019, 27. Mai 2019, S. 5

Elke Steven

Ein Menschenfreund ist gestorben

Nachruf Wolf-Dieter Narr

Am 12. Oktober 2019 starb Wolf-Dieter Narr nach langer Krankheit in Berlin. Wir haben einen Wissenschaftler, Universalgelehrten, einen Pazifisten aus Überzeugung und Menschenfreund verloren. Seine Veröffentlichungen, sein Denken und Wirken können uns lehren, selbst zu denken und Folgerungen für unser Handeln daraus zu ziehen.

Wolf-Dieter Narr lehrte von 1971 bis 2002 als Professor für empirische Theorie der Politik am Otto-Suhr-Institut der Freien Universität Berlin. Er war nicht nur einer der wichtigsten kritischen Sozialwissenschaftler der BRD, sondern vor allem einer der aktivsten Begleiter und Förderer kritischer außerparlamentarischer Bewegungen.

Geboren am 13. März 1937 in Schwenningen am Neckar prägte ihn seine Familiengeschichte im Nationalsozialismus. Seine geliebten Eltern waren selbst tief verstrickt in die nationalsozialistischen Taten. Das führte ihn nach Auseinandersetzungen mit seinem Vater zu immer neuen Reflexionen darüber, zu welchen Verbrechen Menschen in der Lage sind und welche Organisationsformen dem entgegenwirken könnten. Die Fragen nach der gesellschaftlichen Struktur und nach den Bedingungen von gesellschaftlichen Entwicklungen blieben wichtige Themen für ihn: Es gilt zu analysieren, welche Zu- und Umstände den Weg in solche Unrechtsstaaten ebnen. Die Menschen, so fehlbar sie auch sind und handeln, sind verantwortlich, aber sie bleiben Menschen mit Rechten.

Ausgangspunkt seiner Überlegungen waren immer wieder die Menschenrechte, nie gegebene Rechte, die schwierig zu fassen und zu begründen sind. Für das Komitee für Grundrechte und Demokratie, das er mit anderen 1980 gründete, formulierte er: „Wenn wir von Menschenrechten lediglich als einem politischen Konzept sprächen, dann formulierten wir in diesem Falle zu beliebig, zu missverständlich. Wir meinen, ja wir sind davon überzeugt, dass Menschenrechte das politische Konzept darstellen. Das einzige, das systematisch am Gegenpol der Herrschaft verankert ist. Das einzige, das die Menschen, die es betreiben, nicht verdirbt und entfremdet, sondern im nicht endenden Kampf so zu erfüllen vermag, dass sie die Menschenrechte zugleich an sich selber praktizieren."

Seine aus dieser Perspektive folgenden Analysen führten zur radikalen Kritik gegenwärtiger Verhältnisse. Das bleibt so dringlich wie zugleich unpopulär, weil im Sinne der herrschenden Interessen die Menschenrechte funktionalisiert und im Sprachgebrauch relativiert werden. Menschenrechtspolitik muss jedoch radikal, kompromisslos und alles vermeintlich Vorgegebene in Frage stellend sein – oder sie verdient diesen Namen nicht. Wie kaum ein anderer hat Wolf-Dieter Narr über Jahrzehnte für diese materialistisch verstandenen Menschenrechte gekämpft, sie theoretisch begründet und in erforderliche praktische Kritik umgesetzt.

Er lebte, analysierte und forschte nicht im Elfenbeinturm, sondern war immer bei den konkreten Menschen. Für die Menschen, die

Fehlbaren, die Gedemütigten, die, deren Menschenrechte verletzt wurden, setzte er sich unermüdlich ein. Er stritt für die Rechte der Gefangenen, gegen die lebenslange Freiheitsstrafe, aber er besuchte auch Gefangene und blieb mit ihnen im Gespräch. Er setzte sich gegen Zwangsverwahrung in der Psychiatrie ein und verteidigte die Rechte derer, die solche Erfahrungen gemacht haben. Er kämpfte nicht nur gegen die Aushebelung des Grundrechts auf Asyl und für die Rechte der Geflüchteten, er unterstützte diese auch ganz praktisch. Über viele Jahre begleitete und beriet er einen kleinen Altenpflegeverein in Süddeutschland, den er kennen lernte, während er seine alternden Mutter betreute.

Wolf-Dieter Narr war überzeugter Pazifist, das ergab sich aus seiner Analyse gesellschaftlicher Verhältnisse und Strukturen. Vielfältig hat er sich gegen militärische Aufrüstung und Krieg eingesetzt. Als 1999 das vereinigte Deutschland, unter einer rotgrünen Regierung, in den ersten Krieg nach den nationalsozialistischen Verbrechen zog, forderte er mit vielen Freunden und Freundinnen alle Soldaten der Bundeswehr auf, die weitere Beteiligung an diesem Krieg zu verweigern. Die Prozesse wegen Aufrufs zu Straftaten – Fahnenflucht und Gehorsamsverweigerung – gegen die ErstunterzeichnerInnen führten durch alle Instanzen. Letztlich kam es vor dem Berliner Kammergericht zum Freispruch. Die Prozesse boten auch den Rahmen, sowohl gegen diesen Krieg als auch gegen alle Kriege zu argumentieren. Wolf-Dieter Narr begründet in diesem Kontext: „Man muss emotionell und intellektuell lernen – und emotio und ratio sind allemal eng miteinander positiv und negativ verbunden –, schlimme Konflikte und Widersprüche auszuhalten, um einerseits nach den Ursachen zu fahnden und um andererseits nach Lösungen Ausschau zu halten, die mittel- und längerfristig versprechen, weniger Gewalt im Umgang von Menschen mit Menschen in der entsprechenden historischen Situation und ihrem Kontext zu erzeugen. Das ist schwierig."

Als ich Wolf-Dieter 1994 als neue *Sekretärin* des Grundrechtekomitees kennen lernte, übernahm ich schnell die Idee der Demonstrationsbeobachtung und machte sie in enger Kooperation mit Wolf-Dieter Narr zu meiner eigenen Sache. Das war nicht immer leicht neben einem Schwergewicht an Kompetenz, Wissen und Wortgewalt. Schnell verbanden uns die gemeinsamen Erfahrungen bei den Demonstrationsbeobachtungen, auf Feldern oder Straßen stehend, wartend, beobachtend und analysierend, manchmal auch inmitten von Steinhagel und losstürmender Polizei. Immer wieder hat uns die strukturelle und praktische polizeiliche Gewalt empört. Das immer umstrittene, stets gefährdete Grundrecht auf Versammlungsfreiheit erhält seine Besonderheit daraus, dass es ein *kollektives* Grundrecht ist. Bei der Demonstrationsbeobachtung in Heiligendamm anlässlich des G8-Gipfeltreffens hat sich Wolf-Dieter noch am Stock über die Felder gehend beteiligt. Bei der Blockupy Demonstration 2013 in Frankfurt war er noch einmal im Rollstuhl dabei. Da aber mussten wir einsehen und verstehen, wie eingeschränkt, wenn nicht unmöglich die Beobachtung aus dieser Perspektive ist.

Ein anderes Thema, das mich mit Wolf-Dieter Narr verband, war die Auseinandersetzung mit den Entwicklungen im Gesundheitsbereich – von Fragen des Datenschutzes bis zu Fragen nach dem Grundrecht auf körperliche Integrität. Gerade in diesem Kontext wurde oft deutlich, dass er Sprache ausdrucksstark, präzise, aber auch assoziativ und sehr eigen nutzte. So den Menschen zugewandt, wie ich ihn auch noch im Pflegeheim erlebt habe, so ausschließend musste manchmal diese Wortgewalt erlebt werden. Umso trauriger, dass seine Krankheit, die ihm nach und nach die Bewegungsmöglichkeiten nahm, ihm dann auch die Möglichkeit raubte, zu sprechen.

Ich und wir werden ihn vermissen. Aber seine unzähligen Schriften bieten immer neue Ansätze, sich Themen und Fragestellungen zu nähern. So prinzipiell wie Wolf-Dieter Narr sich mit Themen auseinandersetzte, werden die Texte nicht alt. Seine Doktoranden haben in dankenswerte Weise und schwieriger Arbeit seine Schriften gesammelt und zugänglich gemacht: *https://wolfdieternarr.de/*

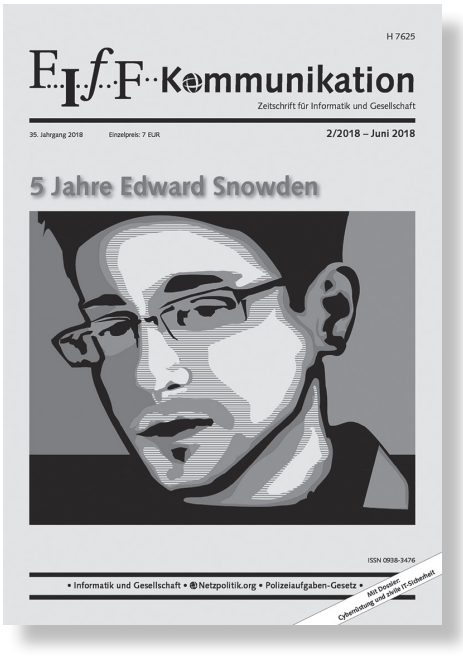
Das FIfF bittet um Eure Unterstützung

Viermal im Jahr geben wir die FIfF-Kommunikation heraus. Sie entsteht durch viel ehrenamtliche, unbezahlte Arbeit. Doch ihre Herstellung kostet auch Geld – Geld, das wir nur durch Eure Mitgliedsbeiträge und Spenden aufbringen können.

Auch unsere weitere politische Arbeit kostet Geld für Öffentlichkeitsarbeit, Aktionen und Organisation. Unsere jährlich stattfindende FIfF-Konferenz, der Weizenbaum-Preis, weitere Publikationen, Kommunikation im Web: Neben der tatkräftigen Unterstützung engagierter Menschen sind wir bei unserer Arbeit auf finanzielle Unterstützung angewiesen.

Bitte unterstützt das FIfF mit einer Spende. So können wir die öffentliche Wahrnehmung für die Themen, die Euch und uns wichtig sind, weiter verstärken.

Spendenkonto:
Bank für Sozialwirtschaft (BFS) Köln
IBAN: DE79 3702 0500 0001 3828 03
BIC: BFSWDE33XXX



Hans-Jörg Kreowski

#FIfFKon19 – Künstliche Intelligenz als Wunderland

Kurze *Rückschau* auf die FIfF-Konferenz 2019 in Bremen

Die FIfF-Konferenz 2019 Künstliche Intelligenz als Wunderland *vom 22. bis 24. November in Bremen ist gerade vorüber. Obwohl der Einreichungsschluss für diese FIfF-Kommunikation lange verstrichen und auch das Layout nahezu fertig ist, habe ich die Gelegenheit zu einem ersten kurzen Vorbericht.*

Als Mitorganisator bin ich sicherlich voreingenommen; aber aus meiner Sicht war die Konferenz sehr erfolgreich. Von den Rückmeldungen her, die mich erreicht haben, sind Programm und Organisation gut angekommen. Fast alles lief nach Plan und wie erhofft, wenn man einmal davon absieht, dass wir den Arbeitsaufwand eher unterschätzt haben.

Das Organisationsteam, zu dem anfangs etwa zehn Personen gehörten und später bis zu fast zwanzig, hat sich erstmals im Juni 2018 getroffen und seit Januar 2019 monatlich. Dass wir thematisch *Künstliche Intelligenz* in den Mittelpunkt rücken, stand frühzeitig fest. Wir haben versucht und wohl auch geschafft, mit den Vorträgen und Arbeitsgruppen ein breites Spektrum an wissenschaftlichen, politischen, wirtschaftlichen, militärischen, gesellschaftlichen und ethischen Fragen und Aspekten abzudecken, die sich um die Künstliche Intelligenz ranken. Unser Ziel war, auf über 100 Teilnehmerinnen und Teilnehmer zu kommen, was mit rund 150 am Freitag und Samstag und 120 am Sonntag unerwartet gut gelungen ist. Vielen Dank an alle, die gekommen sind. Wir hatten sehr viel Hilfe – finanziell, ideell und vor Ort –, wofür wir überaus dankbar sind. Sonst lässt sich eine solche Konferenz auch überhaupt nicht durchführen. Der Platz hier reicht nicht, um alle unterstützenden Organisationen und die helfenden Engel aufzuzählen. Wir bedanken uns auch herzlich bei den Referentinnen und Referenten, die alle ihre Vorträge bestens konzipiert und zur Diskussion angeregt haben, für die allerdings pro Vortrags-Slot zu wenig Zeit war. Schließlich lässt sich noch festhalten, dass die Räume in der Universität Bremen für das Plenum und die Arbeitsgruppen am Samstag und Sonntag und dem Foyer mit den Info- und Verpflegungsständen gut geeignet waren. Dass die Auftaktveranstaltung am Freitag im Übersee-Museum stattgefunden hat, war ebenfalls eine gute Idee.

Es hat in den letzten Jahren ohne Zweifel auf dem Gebiet der Künstlichen Intelligenz (KI) bemerkenswerte und teils auch spektakuläre wissenschaftliche und technologische Erfolge bei Spielen wie Schach, Go, Poker und Starcraft, bei praktischen Anwendungen wie Sprach- und Bildverarbeitung sowie bei der Entwicklung von Robotern gegeben, die tanzen, jonglieren, Fußball spielen, Küchenarbeit verrichten, Pflegeaufgaben übernehmen, chirurgische Eingriffe unterstützen und für Menschen schwer oder nicht erreichbare Orte erkunden und vieles andere mehr können. Wahrlich ein neues Wunderland. Das hat seit einigen Jahren eine besondere Aufmerksamkeit in Politik, Wirtschaft und Medien geweckt. Es vergeht kaum ein Tag, an dem nichts über KI zu sehen, zu hören oder zu lesen ist. Für die Wirtschaft wird die Sicherung der zukünftigen Wertschöpfung durch KI erhofft. Das aktuelle Wissenschaftsjahr ist der KI gewidmet.

Die Bundesregierung hat 2018 eine KI-Strategie auf den Weg gebracht, um den „Weg von *Künstlicher Intelligenz Made in Germany* an die Weltspitze" zu ebnen. Der Bundestag hat mit der Enquête-Kommission *Künstliche Intelligenz – Gesellschaftliche Verantwortung und wirtschaftliche, soziale und ökologische Potenziale* eine breit angelegte Debatte eröffnet. Selbst das kleine Land Bremen steht nicht zurück. Die Bremer Senatorinnen für Wirtschaft und Wissenschaft haben ein Eckpunktepapier für eine *Landesstrategie Künstliche Intelligenz Bremen* erarbeitet. All diese Aktivitäten ordnen sich ein in einen weltweiten geostrategischen Wettlauf um die Führungsrolle in der KI.

Aber sind die hoch gesteckten Erwartungen von Politik und Wirtschaft gerechtfertigt? Oder sind sie übertrieben und gehen in die Irre? Welche Chancen sind mit den aktuellen und zukünftigen Entwicklungen der KI verbunden und unter welchen Bedingungen lassen sie sich zum Nutzen der Menschen umsetzen? Welche Risiken birgt der *Hype* um die KI und wie kann man sie eindämmen oder ganz vermeiden?

Detaillierte Informationen sind weiterhin auf der Konferenz-Webseite *2019.fiffkon.de* zu finden. Ausführlich wird über die Konferenz in der nächsten FIfF-Kommunikation als Schwerpunktthema berichtet mit schriftlichen Fassungen hoffentlich aller Vorträge und mit Berichten aus den Arbeitsgruppen. Die gute Nachricht für alle, die zuhören wollten, aber nicht konnten: Die Video-Mitschnitte der Vorträge werden frei verfügbar auf die Videoportale des Chaos Computer Clubs *media.ccc.de* und Mobile Lecture Uni Bremen *https://mlecture.uni-bremen.de* gestellt. Mit Erscheinen dieser FIfF-Kommunikation ist die Bearbeitung der Videos hoffentlich auch schon abgeschlossen. Sonst bitten wir noch um etwas Geduld.

Der große Knall (2018), Sebastian Hertrich, Foto: Sebastian Hertrich

Dagmar Boedicker

Überwachungs-Gesamtrechnung

Überwachungskompetenzen zwischen Kritik und Gegenwehr

Editorial zum Schwerpunkt

Wir stecken in einem Netz von Überwachungs-Gesetzen auf föderaler, nationaler und internationaler Ebene, das effektiv ermöglicht, „dass sich praktisch alle [unsere] Aktivitäten rekonstruieren lassen." (BVerfG) Wir sind nicht nur einem der vielen Gesetze in der Sicherheits-Architektur oder nur einer Sicherheitsbehörde unterworfen, sondern vielen. Niemand weiß, welche Sicherheitsbehörde auf Basis welchen Gesetzes wann welche privaten Daten abgreifen darf. Eigentlich ein verfassungswidriger Zustand.

Anlass genug für eine Bürgerrechts-Organisation wie das FIfF, das Thema ausführlicher zu beleuchten. In Wirklichkeit haben wir natürlich Expertinnen und Experten gebeten, das für die FIfF-Kommunikation zu tun. Sie haben wirklich Lesenswertes und auch Überraschendes dazu geschrieben. Der Schwerpunkt befasst sich mit dem Wortungetüm Überwachungs-Gesamtrechnung (ÜGR). Nach einer Einführung, die hoffentlich verständlich beschreibt, was eine ÜGR ist, beschreiben PraktikerInnen ihre Erfahrungen damit und ihre Pläne dafür. Das tut zunächst *Angelika Adensamer* von *epicenter.works* in Wien anhand von drei Beispielen – den technologischen Neuerungen, der Größe von Datensets und den privaten Speicherverpflichtungen. Nachdem sie HEAT 1.2 veröffentlicht hatten, arbeiten epicenter.works jetzt an der Version 2 des Handbuchs, das die Debatte über Überwachungsbefugnisse erweitern und mehr Menschen eine Informationsgrundlage geben soll, um sich an dieser Debatte zu beteiligen.[1]

David Leeuwestein hat ein Jahr lang die *Digitalcourage*-Sammlung von Überwachungs-Gesetzen[2] gepflegt. Unter der Überschrift „Kein gutes Jahr" hat er beschrieben, was neu dazu kam, und sein Ausblick auf Bevorstehendes ist nicht gerade optimistisch: „Die nächsten Jahre werden nicht besser". *Digitalcourage* hat Forderungen zu diesem Thema formuliert, wie auch *epicenter.works*.

Frank Herrmann von der *Piraten-Partei* hat sich als Landtags-Abgeordneter in NRW schon 2015 mit diesem Thema befasst. Er kritisiert die Rolle der Parlamente, die leider zu oft die Exekutive nicht ausreichend kontrollieren wollen oder können. Wenn sie dann Anträge in Richtung einer ÜGR stellen, überlassen sie womöglich der Regierung die Bewertung. Herrmann schlägt mit einem zweifelnden Blick auf die Rolle des Bundesverfassungsgerichts (BVerfG) die Brücke von der Praxis zur Theorie.

Die Fachleute entwickeln die Theorie weiter, und dabei kommen überraschende Ansätze heraus. Da das BVerfG den Gesetzgeber zu einer Überwachungs-Gesamtrechnung verpflichtet hat, fragt es sich, wie die denn umzusetzen wäre. In seiner Dissertation (die wir nicht abdrucken) benennt *Tobias Starnecker* relevante Kategorien, die er aus dem Vergleich mit anderen Gesamtrechnungen zieht, der umweltökonomischen Gesamtrechnung (UGR) und der volkswirtschaftlichen Gesamtrechnung (VGR)[3]. *Bieker/Bremert/Hagendorff* hatten schon früher Relevantes zur ÜGR geschrieben.[4] Jetzt haben *Felix Bieker* und *Benjamin Bremert* vom *ULD* mit ihrem Beitrag nachgelegt. Sie kommen zum Ergebnis, dass der EuGH deutlicher als das BVerfG eine Überschreitung des zulässigen Maßes an Überwachung feststellt und untersagt. Kurz und knackig zählen sie die praktischen Fragen auf, denen eine ÜGR begegnet, bis zur Gretchenfrage: Wird der Gesetzgeber Einsicht zeigen? Sie haben Zweifel am Werkzeug ÜGR und setzen auf die Folgenabschätzung als Alternative.

Alternativen schlägt auch Jörg Pohle vor. Für seine Dissertation hatte er schon auf der FIfF-Konferenz 2018 (Thema *Gestaltungsfreiheiten und Machtmuster soziotechnischer Systeme)* den Weizenbaum-Studienpreis als Sonderpreis bekommen. Pohle findet, dass der Begriff der Überwachungs-Gesamtrechnung mehr

verspricht, als er halten kann, dass es sich dabei weder um eine „*Überwachungs*-Gesamtrechnung noch eine Überwachungs-*Gesamt*rechnung noch eine Überwachungs-Gesamt*rechnung*" handele. Ein wesentlicher Kritikpunkt ist, dass wenn immer weitere Bereiche der Gesellschaft verdatet werden sich der Maßstab für Vollständigkeit immer weiter nach oben verschiebt und so den Umfang der existierenden Überwachung relativiert. Sein erster Gegenvorschlag soll den Gesetzgeber zur Durchführung der ÜGR verpflichten, aber nur auf der Basis von Listen von Überwachungsgesetzen und -maßnahmen, die von unabhängigen Dritten erstellt werden. Der zweite, umfassendere, ist die *Freiheitsbestandsanalyse* als konzeptionelles Gegenstück zur ÜGR.

Im letzten Beitrag des Schwerpunkts macht der Anwalt Benjamin Derin deutlich, wieso wir dem Gesetzgeber und der gesamten Politik dringend genauer auf die Finger sehen müssen, mit welchem Instrument auch immer: Sowohl in der Strafprozessordnung als auch in den landesrechtlichen Polizeigesetzen nehmen die Eingriffsermächtigungen zu, kontrolliert werden sie immer weniger. Die Polizeiarbeit erhebt einen neuen Anspruch, relevante Abläufe zu prognostizieren und zu verhindern. Dabei spielt keine Rolle, ob die neuen Überwachungsmaßnahmen überhaupt geeignet sind, irgendetwas zu verhindern, und es ist der Polizei nicht vorzuwerfen, wenn sie ein wenig über das Ziel hinausschießt. Derins Analyse lässt sich untermauern mit dem Zwischenbericht des Forschungsprojekts KviAPol[5]. Er leitet aus seiner Analyse ganz konkrete Forderungen ab.

Wir bedanken uns sehr bei den AutorInnen und KünstlerInnen, die ihre Werke zu diesem Schwerpunkt beigesteuert haben. Und hoffen, dass das sperrige Thema Sie und Euch neugierig macht.

Anmerkungen

1 *https://epicenter.works/sites/default/files/heat_v1.2.pdf und https://epicenter.works/thema/handbuch-ueberwachung (letzter Abruf 31.10.2019)*
2 *https://digitalcourage.de/ueberwachungsgesamtrechnung*
3 *Tobias Starnecker, Videoüberwachung zur Risikovorsorge. S. 371ff*
4 *Bieker F., Bremert B., Hagendorff T. (2018) Die Überwachungs-Gesamtrechnung, oder: Es kann nicht sein, was nicht sein darf.*
5 *Forschungsprojekt „Körperverletzung im Amt durch Polizeibeamt*innen" (KviAPol) am Lehrstuhl für Kriminologie der Ruhr-Universität Bochum, Juristische Fakultät. https://kviapol.rub.de/index.php/inhalte/zwischenbericht (letzter Abruf 31.10.2019)*

Dagmar Boedicker

Überwachungs-Was?

Der Gesichtsausdruck mancher Menschen bei diesem Begriff ist bestenfalls fragend, oft eher so, als hätten sie ihre Ohren blitzschnell auf Durchzug geschaltet und wollten nicht mal wissen, was das eigentlich ist, eine Überwachungs-Gesamtrechnung. Falls es Ihnen und Euch nicht so gehen sollte, dann habe ich eine Chance, wenn ich eine Begriffsbestimmung versuche.

Gesamtrechnungen erheben den Anspruch, alle wesentlichen Einflussgrößen zu erfassen. Das Ergebnis soll eine Aussage über das erlauben, was erhoben wurde, und Vergleiche möglich machen. So fasst die *volkswirtschaftliche Gesamtrechnung* ein Wirtschaftsgeschehen zusammen und zielt auf Vergleiche beispielsweise zwischen Perioden oder Sektoren einer Volkswirtschaft. Ist die Wirtschaft im letzten Jahr geschrumpft? Wie hoch ist die Brutto-Wertschöpfung des Bergbaus im Staat Soundso? Volkswirtschaftliche Gesamtrechnungen sind weder vollständig noch korrekt, trotzdem sind sie Grundlage für Vieles: die Berechnung des Bruttoinlandsprodukts oder des Rentenwerts, Konjunkturmaßnahmen, ...

Eine *Überwachungs-Gesamtrechnung (ÜGR)* fasst alle Befugnisse und Maßnahmen eines Überwachungs-Geschehens zusammen. Und zielt auf den Vergleich zwischen dem, was an Überwachung erlaubt ist, und dem, was unsere Grundrechte unzulässig beschneidet. Wie gefährdet sind unsere Grundrechte, wenn Videoüberwachung im öffentlichen Raum erweitert und mit Gesichtserkennung gekoppelt wird? Dürfen Sicherheitsbehörden auf europäischer, Bundes- und Landesebene weitere Befugnisse zur Überwachung und zum Austausch von Daten erhalten? Können wir noch wissen, wer was über uns weiß, oder ist unsere informationelle Selbstbestimmung längst dahin?

Kann eine ÜGR vollständig und korrekt sein? Sich diesem Ideal wenigstens nähern? Kann sie ein Mittel für die Zivilgesellschaft sein, unser aller Grundrechte zu verteidigen?

Woher kommt der Begriff?

Er wird unserem FIfF-Beirat *Alexander Roßnagel* zugeschrieben[1]. Anlass war das Urteil des Bundesverfassungsgerichts (BVerfG) zur Vorratsdatenspeicherung. In seinem Urteil formuliert das BVerfG, dass „die Freiheitswahrnehmung der Bürger nicht total erfasst und registriert werden darf"[2]. Es verpflichtet den Gesetzgeber zu kontrollieren, dass *die Gesamtheit* von Überwachungs-Maßnahmen diese Grenze des Zulässigen nicht überschreitet. Roßnagel macht deutlich: Es genügt nicht, einzelne Gesetze oder Maßnahmen isoliert auf ihre Grundrechts-Verträglichkeit zu prüfen. Das leistet der Datenschutz im Wesentlichen. Erst wenn wir die Summe all dessen betrachten, was möglich ist, können wir einschätzen, ob es Sicherheit oder Freiheit ist, die da geschützt wird. Und ob es einen Einschüchterungseffekt[3] gibt, der den Boden für autokratische Herrschaft bereiten kann, und unsere Demokratie bedroht.

> *„Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Informationen dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. Wer damit rechnet, daß etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und daß ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte (Art. 8, 9 GG) verzichten."*[4]

Kann/muss eine ÜGR vollständig und korrekt sein?

Ich glaube nicht. Das liegt in der Natur der Sache, weil eine gesamtgesellschaftliche Erhebung zwangsläufig unvollständig bleiben muss. Sie kann nur eine Momentaufnahme sein und es muss Grenzen dafür geben, was in die Aufstellung einfließt und was nicht. Wahrscheinlich ist Mut zur Lücke nötig, schließlich fühlen sich Regierungen und Parlamente durch den Zweck der Terrorabwehr und die öffentliche Sicherheit seit Jahrzehnten legitimiert, immer neue polizeiliche und geheimdienstliche Befugnisse zu erteilen.[5] Ob neue Ermächtigungen wirklich erforderlich sind und die vorhandenen nicht schon ausreichen, prüfen sie dabei nicht. Erst recht wird nicht geprüft, ob das Ausmaß an kumulierter Überwachung bereits bürgerrechtliche Normen verletzt.

Normale Menschen – wir *Betroffene* – können unmöglich einschätzen, in welchem Gestrüpp an Datensammlungen und übermittlungen durch viele Dutzende Behörden ihre informationelle Selbstbestimmung sich verheddert hat.[6] In jedem Bundesland, jedem europäischen Mitgliedstaat sowie auf EU-Ebene gibt es solche Datenbanken, *Interoperabilität* ist angestrebt. Durch dieses Einbinden der anderen Datenbanken beispielsweise ins Schengen-Informationssystem (SIS II) voraussichtlich ab 2020 lässt sich schwer feststellen, unter welchen Voraussetzungen weitere Daten zugänglich werden. SIS II erlaubt den Zugriff auf Gesichtsbilder, DNA-Profile, Handballen- und Fingerabdrücke und verknüpft verschiedene *Ausschreibungen*[7]. Abfragen dürfen die Strafverfolgungs- und Sicherheitsbehörden. Aber nicht nur die. Allein in Deutschland dürfen auf SIS II zugreifen:

- BKA,
- Polizeidienststellen der (16!) Bundesländer,
- Bundespolizeipräsidium,
- Bundespolizeidirektionen,
- Polizei beim deutschen Bundestag,
- Zollkriminalamt,
- Zollfahndungsdienststellen,
- Hauptzollämter,
- Ausländerbehörden der Länder,
- BAMF,
- Bundesverwaltungsamt,
- Generalbundesanwalt,
- Staatsanwaltschaften,
- Kraftfahrtbundesamt,
- Kraftfahrzeugzulassungsstellen.

In Europa gab es schon 2016 zwei Millionen Endnutzer des SIS II. Angesichts der öffentlichen und privaten Datensammelwut fragt es sich schon, wie wir auf die Idee kommen, all dies sei noch demokratisch. Wieso schaudert es uns, wenn wir an chinesische Überwachung denken, aber nicht bei anlassloser Vorratsdatenspeicherung und Kennzeichen-Kontrolle, bei Seehofers Plänen, Kinder vom Verfassungsschutz überwachen zu lassen und die Daten an ausländische Geheimdienste zu übermitteln? Leider stimmt, was Heribert Prantl sagt: „In der Politik der inneren Sicherheit ist es so: Der Quatsch von heute ist das Gesetz von morgen."[8]

Überwachungs-Maßnahmen sind wie Gift. An der Chemikalien-Verordnung *REACH* der EU wurde kritisiert, dass sie nur die einzelnen Giftstoffe ausweist. Man muss aber ihre kombinierte Wirkung im Umfeld der Anwendung betrachten. Wie schädlich etwas ist, ergibt sich aus der Gesamtbetrachtung.

Medien tragen ihren Teil dazu bei, dass die umfassende Kontrolle EU-weit gerechtfertigt wird durch Terrorismus, Großrisiken und Verbrechensfurcht. Das sollte uns nicht davon ablenken, dass die Wurzel der Sicherheitspolitik ein allgemeines Kontrollbedürfnis ist. Gesetzgeber neigen dazu,

> *„[...] Verbrechensfurcht zuerst zu schüren und sie dann zu bedienen, im Spannungsverhältnis von Freiheit und Sicherheit die Sicherheit stark zu machen, Gefahrenszenarien zu pflegen und mit Gesetzesvorlagen zu garnieren, die Grundrechte zu verschatten und Sonderstrafrechte für gefährliche Täter auszuarbeiten [...]"*[9]

Gleichzeitig fehlen Kontrollmöglichkeiten für die Zivilgesellschaft. Datenschutz-Folgenabschätzungen sieht die Datenschutz-Grundverordnung (DS-GVO) zwar vor, sie scheinen aber ebenfalls zu fehlen. Regierungen verstecken Überwachung erfolgreich vor parlamentarischer und zivilgesellschaftlicher Kontrolle.[10]

Wenn wir wissen wollen, was der Staat über uns weiß, brauchen wir Bürgerinnen und Bürger Hilfe. Die brauchen auch die unermüdlichen Parlamente und Ministerien. Wir brauchen so etwas wie eine Überwachungs-Gesamtrechnung, um zu erfahren, ob nicht etliche Maßnahmen abgeschafft werden müssen, bevor neue hinzukommen dürfen.

Foto vom 34. Kongress des CCC (2017), Plakate laquadrature.net

Was gehört in eine ÜGR?

Diese Fragen sollte die ÜGR beantworten: Wer weiß was über die Menschen in Deutschland? Welche Folgen hat dieses Wissen für die Betroffenen und die demokratische Gesellschaft? Gilt die Unschuldsvermutung noch? Wie effektiv ist die Überwachung? Bringen die Einschränkungen von Freiheit und Privatsphäre so viel Sicherheit, dass sie die Einbußen aufwägen? Welche Wirkung haben technische Entwicklungen wie wachsende Speicher- und Rechenkapazitäten, Künstliche Intelligenz und zunehmende Verknüpfbarkeit von Systemen? Wird die Gefahrenabwehr zur Gefahr? Muss der Gesetzgeber Überwachungs-Maßnahmen rückgängig machen?

In seiner Dissertation „Videoüberwachung zur Risikovorsorge" führt Tobias Starnecker wesentliche Aspekte auf, er stützt sich dabei auf Autoren zum Thema Vorrats-Datenspeicherung.[11]

Wenn das BVerfG urteilt, dass „die Freiheitswahrnehmung der Bürger nicht total erfasst und registriert werden darf“[12], sei das eher als ein Verbot umfassender gesamtgesellschaftlicher Überwachung zu verstehen. Ziel sei es, den Umbau der Sicherheitsarchitektur zum grenzenlosen Präventionsstaat zu hemmen, auch wenn die Gefahrenvorsorge unerlässlich sei. Das BVerfG gebe Gestaltungsspielraum, weiche dabei aber nicht ab von den Prinzipien des Rechts auf informationelle Selbstbestimmung, dem Zweckbindungsgrundsatz und dem Verhältnismäßigkeitsprinzip.

Zu erfassen und beurteilen seien der Stand staatlicher Überwachung, die Verhältnismäßigkeit der konkreten Überwachungsinstrumente und dann die Gesamtbelastungen bürgerlicher Freiheiten durch alle staatlichen Überwachungs-Maßnahmen. Nicht für das Individuum, sondern für alle Betroffenen mit ihren diversen Lebensweisen und Lebensbedingungen.

- **Welche Daten erhebt und verarbeitet der Staat?**
  Es geht um mehr: nicht nur darum, welche Daten der Staat erhebt und verarbeitet, sondern auch um Stand und Entwicklung von Technik und Gesellschaft. Davon hängt schließlich ab, mit welcher Technik Datenbanken verarbeitet werden, ob beispielsweise Daten aus der Video-Überwachung von einer Polizistin ausgewertet werden oder massenhaft mit selbstlernender Software. Ob eine Gesellschaft fast flächendeckend verwanzt ist und über ihre Smartphones und im Austausch über *soziale* Medien Datenspuren hinterlässt, die breiter sind als das Kielwasser eines Ozeandampfers. Ein Blick in zufällig ausgewählte Gesetze wie das G 10[13], das TMG[14], BKAG[15] oder das Bayerische Polizeiaufgaben-Gesetz zeigt, dass die Erhebung unterschiedlich und für Nicht-Juristen unübersichtlich geregelt ist. Die Strukturen der Gesetze sind verschieden, die vom Gesetz Betroffenen können unterschiedlich sein (Dritte, Zielpersonen, ...), und es ist nicht einfach ersichtlich, welche Daten erhoben werden. Für die Betroffenen also wenig erhellend!

- **Welche präventiven und repressiven Befugnisse hat der Staat, wie häufig setzt er sie ein und wie kombiniert er sie?**
  Jede Behörde hat ihr eigenes Gesetz, oft mit Bezügen zu weiteren Gesetzen. Nicht selten bestehen sie hauptsächlich aus Verweisen auf andere Gesetze. Normenklarheit sieht anders aus. Wie oft die Behörden ihre Befugnisse ausüben und wie das Zusammenspiel von Behörden aussieht, darüber erfahren wir so gut wie nichts, Statistiken über die Anwendung werden selten erhoben. Schon gar nicht von unabhängiger Seite.

- **Auf welche privaten Datenbestände hat der Staat Zugriff?**
  Inzwischen spielt es keine Rolle für die umfassende gesamtgesellschaftliche Überwachung, ob der Staat oder Private sie vornehmen. Gesetze erlauben den Zugriff auf private Datenbanken durch Verfassungsschutz, Nachrichtendienste oder die Polizei.

Starnecker kommt zu dem Schluss, dass der Staat prüfen muss, ob er durch neue Regelungen im Bereich des Sicherheitsrechts nicht die rote Linie zu einer umfassenden gesamtgesellschaftlichen Überwachung überschreitet. Vorgeschaltet sei eine Beobachtungspflicht, damit er dieser Prüfpflicht ordnungsgemäß genügen kann, beispielsweise durch empirische Untersuchungen wie soziologische Studien. (Einschüchterungs- oder Anpassungseffekte können Juristinnen und Juristen nicht beurteilen.) Dieser Verpflichtung müsse der Gesetzgeber kontinuierlich nachkommen. Neben Prüfungs- und Beobachtungspflicht ergebe sich noch eine Abstimmungspflicht auf europäischer Ebene.

Bei einer solchen Prüfung ist zwischen anlassloser Überwachung und solcher zu unterscheiden, die gezielt Personen überwacht, bei denen womöglich Anlass zur Vorsicht besteht. Es gibt begründete Zweifel an der Wirksamkeit anlassloser Beobachtung zur Prävention.[16] Schnell wird der Heuhaufen zum Selbstzweck und die Nadel drin nicht gefunden. Dagegen kann diese massenhafte Überwachung gerade die Menschen einschüchtern, auf die unsere Demokratie besonders angewiesen ist: politisch Engagierte, Gewerkschaftsmitglieder, ehrenamtlich Aktive und andere. Vor allem verwundbare Menschen sind gefährdet, beispielsweise mit anderer Hautfarbe oder Geflüchtete. Sie müssen Diskriminierung und ihre Folgen fürchten, ebenso wer sich mit ihnen solidarisiert.

Lässt sich eine ÜGR umsetzen?

Wenn der politische Wille besteht, könnte eine wissenschaftliche Einrichtung in interdisziplinärer Zusammenarbeit diese Bestandsaufnahme sehr wohl leisten. Bisher findet das aber nicht statt.

> *„Bisher hat der Bundestag nur eine Übersicht der Gesetzgebung zur Speicherung von personenbezogenen Daten zusammenstellen lassen, wobei die einzelnen Gesetze lediglich in ein bis zwei Sätzen erläutert werden.[17] Es erfolgt insbesondere keinerlei Bewertung der durch die Gesetze erfolgenden Grundrechtseingriffe.“[18]*

Solche knappen Übersichten schreiben Juristen für Juristen. Für Laien sind sie nutzlos. Auf der anderen Seite gibt es die umfangreichen Stellungnahmen, die bei Gesetzesänderungen (und Verschärfungen des Überwachungsdrucks) den Parlamenten vorgelegt werden. Zwar verweisen ihre Verfasser regelmäßig auf vorhandene Regelungen in anderen Gesetzen und darauf, wie sie verfassungsrechtlich einzustufen sind, normalen Menschen hilft das aber nicht weiter. Die haben keine Zeit, sich durch teils gegensätzliche Bewertungen und Verweisungsdschungel zu kämpfen. Wer versucht hat, beispielsweise eins der derzeitigen Vorhaben zu den Polizeigesetzen der Länder einzuschätzen, weiß, was ich meine. Auch wenn Datenschutz-ExpertInnen den Staats- und Verfassungsrechtlern zur Seite stehen, bietet ihre Expertise für Laien nur wenig Hilfe. Sie prüfen, ob die Schutzziele der informationellen Selbstbestimmung gewährleistet sind: Datenminimierung als allgemein gültiges Ziel, Verfügbarkeit, Integrität, Vertraulichkeit, Transparenz, Intervenierbarkeit, Nicht-Verkettung von personenbezogenen Verfahren.[19] Laien dürften diese Ziele arg technisch vorkommen. Und was bedeutet eigentlich Verhältnismäßigkeit in der Beziehung zwischen Bürgern und Sicherheitsbehörden? Das liegt im Auge der Betrachterin. Wie viele Engagierte in Nichtregierungs-Organisationen wie CILIP, Digitalcourage, FIfF und anderen arbeiten sich auch die DatenschützerInnen an einzelnen Maßnahmen ab.

Juristen allein können die ÜGR nicht stemmen. Es gehört technischer Sachverstand ins interdisziplinäre Team, um einschätzen

zu können, wie Fortschritte in Informations- und Kommunikationstechnik die Überwachung beeinflussen und ob neue Risiken durch sie entstehen. Betroffene können nicht beurteilen, ob sich eine neue Qualität der Überwachung bildet, wenn Datenbestände verknüpft oder durch raffiniertere Software verarbeitet werden. Es mag effizienter sein, den Heuhaufen durch maschinelles Lernen zur automatisierten Musteranalyse und Anomalie-Erkennung zu durchwühlen, es werden unter den Treffern aber auch immer mehr falsche Funde sein. Das kann jede/n treffen. Neue Sicherheitsrisiken entstehen durch unzureichend geschützte Datenbanken oder Übertragungswege.

Kriminologinnen und Kriminologen können die Effektivität der Maßnahmen beurteilen. Sie müssten sich damit befassen, wie viele schwere Straftaten verhindert, wie viele Verbrecher gefasst und wie oft im Vergleich dazu bestimmte Maßnahmen eingesetzt wurden. Bisher gibt es wenig mehr als die Polizeiliche Kriminalstatistik (PKS). Sie ist kaum geeignet, die Verhältnismäßigkeit von intensiven Grundrechtseingriffen zu beurteilen. Für eine ÜGR kann die Kriminalwissenschaft hoffentlich die Argumente der SicherheitspolitikerInnen gerade rücken, die uns Folgendes vermitteln:

> *„Was ist der Datenschutz, so legen sie nahe, was ist die Trennung von Polizei, Geheimdiensten und Militär, was sind Unschuldsvermutung oder die Bestimmtheit von Tatbeständen denn wert angesichts schrecklicher Gefahren für viele Menschen durch einen Bombenanschlag, der Tötung eines wehrlosen und unschuldigen Kindes durch seinen Entführer, eines historischen Chaos bei der WM?"*[20]

Da hängt es oft von Verwaltungsgerichten ab, ihnen in den Arm zu fallen. Winfried Hassemer

> *„[...] beobachte[t] mit Sorge, mit welchen argumentativen Schleifen die Verwaltungsgerichte den Datenschutz zu retten versuchen gegenüber einer ‚abstrakten Gefahr' durch die Aktivierung von terroristischen ‚Schläfern' – eine Gefahr, für deren wirklichkeitsnahe Beurteilung ihnen doch keine tauglichen Instrumente zur Verfügung stehen und die sie gleichwohl professionell abschätzen müssen."*[21]

Schließlich müssen SozialwissenschaftlerInnen mitarbeiten. Sie sind kompetent dafür, Verhalten empirisch zu erfassen, den Einfluss der Maßnahmen systemisch zu beurteilen und mögliche Trends zu erkennen.

Auf den interdisziplinären Kriterienkatalog für die Evaluation dürfen wir gespannt sein.

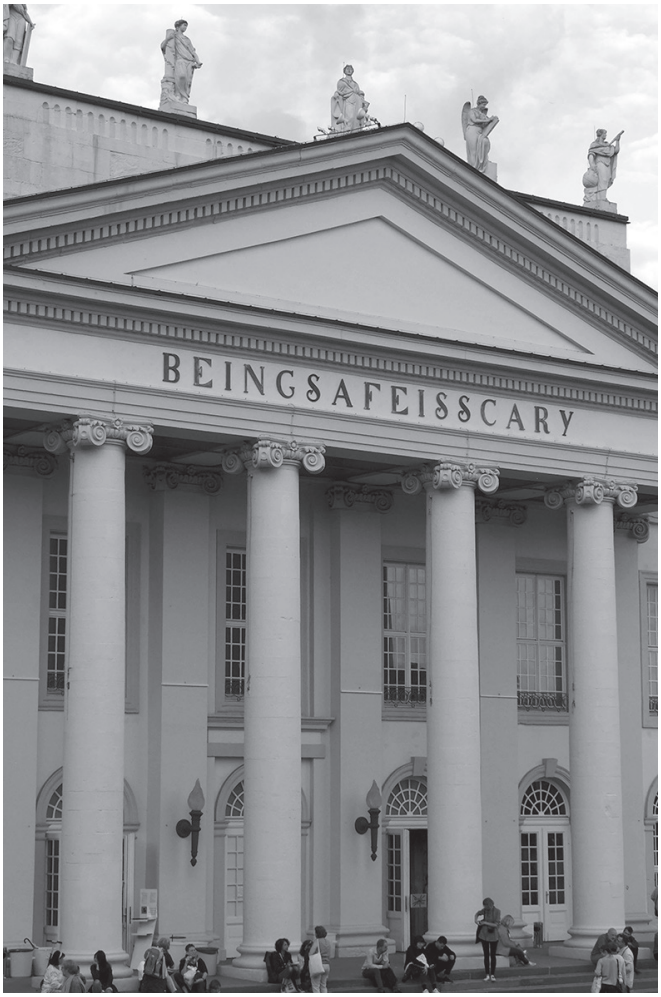
Kann eine ÜGR unserer Demokratie helfen?

Eigentlich wissen wir alle, dass die Demokratie kein Selbstläufer ist. Damit sie lebt und stark ist, auch gegen ihre Widersacher, müssen ihre Bürgerinnen und Bürger mitarbeiten. Viele! Nach dem Motto „Jeder für sich" kann es nicht funktionieren. Wir erleben aber seit Jahren, wie Hass und Hetze lautstark und gewalttätig *aufTrumpen,* wie Feindbilder geschaffen werden und die Gesellschaft in ein *Wir* und ein *Die* spalten. Solidarität wirkt wie ein Begriff aus dem vergangenen Jahrhundert.

> *„Schon sehr früh in der Sozialdemokratie hat sich diese Klassensolidarität zu einer allgemeinen Gesellschaftssolidarität erweitert. Man wollte nicht nur Lösungen für die Arbeiter suchen, sondern man wollte Lösungen, die allen Menschen passen könnten, suchen. Und wir sagen auch heute so: Wenn eine Gesellschaft zusammenhalten soll, so muss es eine Solidarität in der Gesellschaft geben."*

Das hat Olof Palme gesagt.[22] Die Zeiten waren andere, Misstrauen und Überwachung spielten damals in Schweden keine große Rolle. Heute fehlt vielen Menschen das Vertrauen in ihre Institutionen, vor allem in die Politik, die als *Establishment* diffamiert wird und daran gewiss nicht unschuldig ist. Es ist aber verheerend, wenn Menschen mehr Vertrauen in Sicherheitsapparate haben als in ihre Abgeordneten. Nein, Sicherheit ist nicht das oberste Grundrecht, wie ein Innenminister fälschlich behauptet hat. Die Menschenwürde ist Basis aller Rechte, sie zu achten und zu schützen ist Verpflichtung aller staatlichen Gewalt. Dabei müssen wir der staatlichen Gewalt behilflich sein, wenn sie sich auf den Holzweg begeben hat.

So wenig wie Strafe oder Abschreckung Sicherheit schaffen[23], so wenig tut es Überwachung als Prävention. Abstrakte Gefährdungsdelikte, verdeckte und massenhafte Beobachtung (vulgo



Being Safe Is Scary, Foto von der documenta 14 (2017)

Schnüffelei) und Erfassung schaffen keine Sicherheit. Wie Winfried Hassemer in seinem Beitrag *Sicherheit durch Strafrecht* feststellt:

> *„Prävention und Gefahrenabwehr hingegen sind prinzipiell schrankenlos, wie man in der Theorie leicht zeigen und in der Praxis oft beobachten kann."*[24]

Eine ÜGR sollte uns allen ein Urteil darüber ermöglichen, ob eine Gesellschaft nicht ganz andere als Überwachungs-Maßnahmen benötigt, wenn ihre Wählerinnen und Wähler sich so unsicher fühlen, dass sie dem Gesetzgeber ohne Widerworte immer weiter gehende Werkzeuge durchgehen lassen. In jedem Fall sollte die ÜGR uns einen Überblick ermöglichen und Klarheit über den Überwachungsdruck und die Rechtslage geben. Wir müssen selbst einschätzen können, wie sehr Überwachung in die Privatsphäre eingreift und ob die rechtsstaatlichen Schutzmaßnahmen für unsere Freiheit ausreichen. Weil wir das Gesamtbild nicht kennen, glauben wir, unsere Welt der Datennutzung sei demokratisch und transparent. In Wirklichkeit sind wir vermutlich sehr nah an US-amerikanischen oder chinesischen Verhältnissen. Wenn wir uns über repressive Maßnahmen der Volksrepublik China gegenüber ihrer uigurischen Bevölkerung aufregen, übersehen wir die Überwachung in der EU von Geflüchteten oder Menschen, die aus anderen Gründen ins Raster fallen. Es muss nicht erst zu Repression kommen, schon die Überwachung verstößt gegen die Menschenwürde.

Nachtrag und Richtigstellung zu meinem Beitrag ...

... und vielen Dank an den kritischen Leser David, der mich freundlich auf einen Fehler hingewiesen hat. In „Leerstelle in der legislativen Praxis" in der FIfF-Kommunikation 1/2019 hatte ich behauptet, dass im SIS alle Grenzübertritte und die Daten der Verkehrskontrolle aus dem erfundenen Beispiel vermerkt seien. Tatsächlich bietet SIS im Rahmen der Interoperabilität bisher wohl nur im Fall einer verdeckten Beobachtung den Zugang zu separaten europäischen Datenbanken von nationaler Polizei und Justiz. Im SIS selbst stehen sie nicht. Zukünftig werden sie über den gemeinsamen Identitätsspeicher erreichbar sein.

Definition

> *„Der additive Grundrechtseingriff ist [...] eine Einzelfallbetrachtung unter Einbeziehung weiterer konkreter staatlicher Maßnahmen, die ebenfalls den Betroffenen treffen."*
> Tobias Starnecker, Videoüberwachung zur Risikovorsorge. S. 371ff

Anmerkungen

1 *Roßnagel A (2010) Die „Überwachungs-Gesamtrechnung" – Das BVerfG und die Vorratsdatenspeicherung, NJW 2010, 1238*
2 *BVerfGE 125, 260, Rn. 218 (Vorratsdatenspeicherung)*
3 *chilling effect*
4 *BVerfGE 65, 1 (43).*
5 *Zwischen 2010 und 2017 hat allein der Bundestag rund 40 neue Überwachungs- und Sicherheitsgesetze beschlossen. Von den gesetzgeberischen Aktivitäten der Bundesländer für ihre Polizeien, Landeskriminal- und Verfassungsschutz-Ämter ganz zu schweigen. Siehe https://digitalcourage.de/ueberwachungsgesamtrechnung (letzter Zugriff 31.10.2019)*
6 *Grob geschätzt gibt es 50 bis 80 Gesetze, die den unterschiedlichsten Sicherheitsbehörden auf mehreren Ebenen eine teils anlasslose Überwachung gestatten.*
7 *Ausschreibungen gibt es in polizeilichen Informationssystemen, beispielsweise im Schengen Informationssystem (SIS). Sie können Sachen oder Personen betreffen und enthalten „die Daten, die erforderlich sind, um die Identität oder den Aufenthaltsort einer Person festzustellen oder einen Gegenstand ausfindig zu machen und eine geeignete operative Maßnahme zu ermöglichen." (COM(2016) 883 final 2016/0409 (COD)) Zu den operativen Maßnahmen gehören Festnahme, Aufenthaltsermittlung, Beobachtung, Fahndung, Rückführung Geflüchteter, ...*
8 *Süddeutsche Zeitung vom 3./4.8.2019*
9 *Hassemer W: Sicherheit durch Strafrecht, S. 18*
10 *https://www.sueddeutsche.de/politik/seehofer-datenaustauschgesetz-1.4479069; https://www.sueddeutsche.de/politik/staatstrojaner-seehofer-ueberwachung-1.4564648 (letzter Zugriff 30.10.2019)*
11 *Starnecker T: Videoüberwachung zur Risikovorsorge. S. 367ff*
12 *BVerfG, Urteil vom 2.3.2010, NJW 81 (2010), 833, 839*
13 *Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10-Gesetz – G 10)*
14 *Telemediengesetz (TMG)*
15 *Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten (Bundeskriminalamtgesetz – BKAG)*
16 *Bergen P, Sterman D, Schneider E, Cahall B (2012) Do NSA's Bulk Surveillance Programs Stop Terrorists? New America Foundation, www.newamerica.net (zuletzt aufgerufen am 18.1.2014)*
17 *Wissenschaftlicher Dienst des Deutschen Bundestags, Sachstand – Gesetzgebung zur Speicherung von personenbezogenen Daten, WD 3 – 3000 – 089/16 vom 15.3.2016.*
18 *Bieker F, Bremert B, Hagendorff T (2018) Die Überwachungs-Gesamtrechnung, oder: Es kann nicht sein, was nicht sein darf. Roßnagel A et al. (Hrsg.), Die Fortentwicklung des Datenschutzes, DuD-Fachbeiträge, https://doi.org/10.1007/978-3-658-23727-1_8*
19 *Datenschutz-Grundverordnung Art. 5*
20 *Hassemer W: Sicherheit durch Strafrecht, S. 18f*
21 *a.a.O., S. 26f*
22 *zitiert nach einem Beitrag von Matthias Bertsch im DLF vom 14.10.2019*
23 *Wofür die USA ein abschreckendes Beispiel bieten, wie auch Brasilien oder die Philippinen.*
24 *Hassemer W: Sicherheit durch Strafrecht, S. 27*

Dagmar Boedicker

Dagmar Boedicker ist Journalistin, technische Redakteurin und langjährige Redakteurin der FIfF-Kommunikation.

Angelika Adensamer

Aspekte einer Überwachungs-Gesamtrechnung

Eine Überwachungs-Gesamtrechnung ist notwendig, weil die Betrachtung der einzelnen gesetzlichen Überwachungsbefugnisse alleine nicht ausreichend Aufschluss über die Lage der Freiheitsrechte und Achtung der Privatsphäre geben kann. Dies wird anhand von drei Beispielen konkretisiert: 1. technologische Neuerungen, 2. die Größe von Datensets und 3. private Speicherverpflichtungen. Die Ausweitung staatlicher Überwachung erfolgt nicht allein durch die Ausweitung der gesetzlichen Ermittlungsbefugnisse. Auch technische Entwicklungen und Speicherverpflichtungen und -praktiken müssen in der Evaluierung von Überwachungsbefugnissen eine Rolle spielen und unter Umständen zu ihrem Rückbau führen.

Als Grundrechtsorganisation ist epicenter.works die Kontrolle der staatlichen Überwachungsbefugnisse und ihre Beschränkung auf das absolut Notwendige ein großes Anliegen. Daher haben wir schon 2016 einen ersten Aufschlag für eine Anleitung zur Überwachungs-Gesamtrechnung im Handbuch zur Evaluation der Anti-Terror-Gesetze in Österreich (HEAT)[1] *gemacht. Drei Jahre später überarbeiten wir dieses nun, um es verständlicher und lesbarer als „Handbuch Überwachung" aufzubereiten. Das* Handbuch Überwachung *soll einen Überblick über alle polizeilichen Überwachungsbefugnisse geben: die Voraussetzungen ihres Einsatzes, ihre Geschichte, politische Kontroversen, die sich um sie entsponnen haben, ihren Grund- und Datenschutz- sowie EU-rechtlichen Rahmen, bis hin zu dem, was wir über die Häufigkeit ihres Einsatzes und ihre Effektivität wissen. Auch neuere Überwachungstechnologien, ihr Einsatz in Österreich und ein Ausblick darauf, was noch auf uns zu kommen könnte, werden darin Platz finden. Die Zielgruppe des Handbuchs sind einerseits alle interessierten Menschen, die sich mehr in die Debatte über staatliche Überwachung einbringen möchten, aber davor zurück schrecken, weil das Thema eher unübersichtlich und kompliziert ist. Andererseits soll es auch eine Hilfestellung sein für Menschen, die zu dem Thema arbeiten ohne Rechtswissenschaften studiert zu haben, beispielsweise Journalisten und Journalistinnen oder Politikerinnen und Politiker.*

Das Handbuch soll die Debatte über Überwachungsbefugnisse erweitern und mehr Menschen eine Informationsgrundlage geben, um sich an dieser zu beteiligen. Außerdem soll das Handbuch eine Grundlage für eine Überwachungs-Gesamtrechnung darstellen, um die Politik dazu zu bewegen, sich einen Überblick über das Ausmaß staatlicher Überwachung, ihre Notwendigkeit und ihre Grundrechtskonformität zu verschaffen. Dies soll geschehen, bevor Überwachungsbefugnisse immer weiter ausgeweitet werden, und soll letztendlich in Bereichen, wo sie überschießend und unverhältnismäßig sind, auch zu einem Abbau der Überwachungsbefugnisse führen.

Das Konzept der Überwachungs-Gesamtrechnung geht auf ein Urteil des deutschen Bundesverfassungsgerichts aus 2010 hervor, in dem der Gesetzgeber „in Blick auf die Gesamtheit der verschiedenen schon vorhandenen Datensammlungen zu größerer Zurückhaltung" angehalten wird.[2] Eine Überwachungs-Gesamtrechnung ist also deswegen notwendig, weil die Betrachtung der einzelnen gesetzlichen Überwachungsbefugnisse alleine nicht ausreichend Aufschluss über die Überwachungssituation und im Umkehrschluss über die Lage der Freiheitsrechte und Achtung der Privatsphäre geben kann. Ich möchte diesen Gedanken im Folgenden anhand von drei Problemfeldern konkretisieren: Das erste betrifft die Ausweitung von Überwachungsbefugnissen durch technologische Neuerungen, das zweite die Größe von verarbeiteten Datensets und das dritte Speicherverpflichtungen, die polizeiliche oder nachrichtendienstliche Abfragen ermöglichen.

1. Ausweitungen von Überwachungsbefugnissen durch technologische Neuerungen

Technischen Fortschritt nutzen auch die Ermittlungsbehörden, und dies oftmals, ohne dass für den Einsatz neuer Überwachungstechnologien auch neue und eigene gesetzliche Befugnisse geschaffen werden. Die neuen Technologien werden auf Basis alt hergekommener Rechtsgrundlagen eingesetzt, obwohl die neuen Überwachungstechnologien die Grundrechtseingriffe massiv verstärken. Oft wird in diesem Zusammenhang von „Technologieneutralität" der Rechtsgrundlagen gesprochen, beispielsweise im Bezug auf die Strafprozessordnung in den Materialien zum Überwachungspaket, das 2018 die Überwachungsbefugnisse in Österreich massiv ausweitete[3]. Der Begriff der Technologieneutralität ist aber im Hinblick auf die veränderte Intensität der Grundrechtseingriffe irreführend.

Es ist eine durch die Menschenrechte garantierte Voraussetzung, dass bei der Einführung von Überwachungsbefugnissen eine Einschätzung darüber zu treffen ist, ob ihr Nutzen im Verhältnis zu ihrer Eingriffsintensität steht (Verhältnismäßigkeitsprüfung). Ändert sich im Nachhinein aber die Eingriffsintensität der Befugnis, kann sich auch das Ergebnis der Verhältnismäßigkeitsprüfung ändern und die Befugnis somit grundrechtswidrig werden. Aus diesem Grund wäre eine regelmäßige systematische Überprüfung der Recht- und Verhältnismäßigkeit der Überwachungsmaßnahmen notwendig. Unter Umständen müssen diese dann eingeschränkt, eingestellt oder abgeschafft werden. Die Ausweitung von Befugnissen durch neue Technologien lässt sich anhand folgender Beispiele illustrieren: 1. Automatische Gesichtserkennung, 2. Drohnen zur Videoüberwachung und 3. *Predictive Policing.*

Im April 2019 wurde bekannt, dass die österreichische Polizei plant, ab Dezember desselben Jahres, Software zur *automatischen Gesichtserkennung* einzusetzen.[4] Eine neue gesetzliche Grundlage ist dafür nicht vorgesehen, sondern die neue Analysesoftware soll auf Basis allgemeiner sicherheitspolizeilicher Bestimmungen verwendet werden.[5] Die Software soll Standbilder aus Videoüberwachungsmaterial berechnen, die das Gesicht einer verdächtigen Person zeigen und diese maschinell mit Bildern der polizeilichen erkennungsdienstlichen Datenbank abgleichen. Es wird davon ausgegangen, dass dieses Abgleichdatenset ein bis fünf Millionen Datensätze umfasst.[6] Es liegt auf der Hand,

dass ein automatischer Abgleich mit Millionen von Gesichtern eine andere Dimension eines Grundrechtseingriffs darstellt als die menschliche Datenauswertung.

In Österreich werden zur Zeit in einer Pilotphase erstmals 76 *Drohnen* zur polizeilichen Videoüberwachung – unter anderem zur Überwachung von Versammlungen – eingesetzt, und dies ohne neue Rechtsgrundlage[7]. Auch in Deutschland wird der Einsatz von Drohnen durch die Polizei diskutiert.[8] Der Einsatz von Drohnen verändert die polizeilichen Befugnisse zur Videoüberwachung maßgeblich. Drohnen sind beweglicher als heute noch üblichere Stand- und Mastkameras. Das bedeutet, sie können aus anderen Perspektiven filmen, beispielsweise in Privatwohnungen hinein. Außerdem ist es weitaus schwieriger, einer Drohne bewusst auszuweichen, als es bei weniger beweglichen Kameras möglich ist.

Eine weitere technologische Veränderung althergebrachter Polizeibefugnisse stellt *Predictive Policing* dar. Um ihre Arbeit „vorhersehend" zu gestalten, verarbeitet die Polizei je nach Programm große Mengen personenbezogener Daten, Daten über Kriminalitätsaufkommen u. ä. In Österreich ist derzeit ein Programm in Betrieb, das der Vorhersage von Wohnraumeinbrüchen dienen soll.[9] In die Gebiete, die durch das Programm als besonders gefährdet gekennzeichnet werden, fahren Streifendienste öfter zur Prävention. Dadurch erlangt die einfache Befugnis des Streifendienstes eine völlig neue Bedeutung, die neue Fragen, wie nach Diskriminierung durch Algorithmen, Verantwortlichkeit, Transparenz und Kontrolle aufwirft. Solche Systeme wirken zurück auf die Datenbasis auf der sie funktionieren. Es kann beispielsweise sein, dass man aus den Gebieten, in denen öfter kontrolliert wird, mehr Daten über „verdächtige" Merkmale bekommt, die dann wiederum die Basis für weitere Kontrollen werden. Das würde eine Rückkoppelungs-Schleife erzeugen. Die Frage, was ein Streifendienst eigentlich bewirkt, und ob er das richtige Mittel zur Bekämpfung von Wohraumeinbruch ist, wird dabei überhaupt nicht mehr gestellt.

Auch das System der *Fluggastdatenverarbeitung,* die aufgrund einer EU-Richtlinie[10] für alle Mitgliedstaaten verpflichtend ist, birgt eine Form des *Predictive Policing*. Laut Erwägungsgrund 7 der Richtlinie sollen die Daten unter anderem dazu dienen, Personen zu ermitteln, die bis dahin nicht verdächtig waren. In diesen Datenbanken mit Daten von Millionen Menschen[11] wird also erstmals ohne vorherigen Verdacht mittels *Data Mining* erst Verdacht generiert, das heißt die Polizei wird völlig unabhängig davon tätig, ob ein Verbrechen geplant wird oder begangen wurde. So verändert sich die Polizeiarbeit durch den Einsatz von Algorithmen grundlegend.

Diese Ausweitungen von Überwachung durch neue technologische Möglichkeiten sind ohne demokratische Beschlüsse und damit weitgehend auch ohne breite gesellschaftliche Debatte nicht vertretbar.

2. Größe der Datensets und zunehmende Prävalenzfehler

Mit der zunehmenden Größe von Datensets im Zeitalter von Massenüberwachung und *Big Data* bei gleichbleibender (in Österreich aktuell sogar sinkender Kriminalitätsrate) nimmt auch die Gefahr für alle Menschen zu, selbst als falsche Treffer *(false positives)* eingestuft zu werden. Die Vergrößerung der Datensets mit denen gearbeitet wird, verschlechtert die Effizienz von Überwachungsmaßnahmen, statt sie zu verbessern oder auch nur neutral zu skalieren. Der für viele Menschen intuitiven Annahme, mehr Daten seien immer besser, liegt der sogenannte Prävalenzfehler *(Base Rate Fallacy)* zugrunde. Dieser Fehler besteht darin, dass einer relativen hohen Treffsicherheit vertraut wird, ohne die zugrunde liegende Wahrscheinlichkeit eines Treffers im gesamten *Sample* zu beachten.[12]

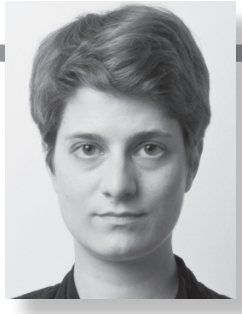
Auch bei guter Trefferquote wird es zu einer sehr hohen Rate an falschen Treffern kommen, wenn in einem sehr großen Datenset (wie den Fluggastdaten) nach einem sehr seltenen Ereignis gesucht wird (beispielsweise Terroranschlägen). Jeder falsche Treffer bedeutet, dass eine Person genauer überwacht wird, die sich nichts zu Schulden kommen hat lassen. Die Wahrscheinlichkeit wird also immer höher, ungerechtfertigt ins Visier zu kommen. In Österreich hielten in den ersten acht Monaten des Fluggastdatensystems nur 0,15 % aller 190.541 Treffer einer genaueren Überprüfung stand[13] und auch in Deutschland geht man nur von 0,1 % korrekten Treffern aus.[14]

Da wegen der fortschreitenden Digitalisierung immer mehr Daten über alle Lebensbereiche der Menschen vorliegen und diese immer häufiger gesamt und automatisch analysiert werden, um auf Basis von Algorithmen Entscheidungen zu treffen, werden auch die falschen Treffer zunehmen und mehr und mehr Menschen von den Folgen betroffen sein.

3. Interaktion von Speicherverpflichtungen mit polizeilichen Abfragen

Speicherverpflichtungen Privater, insbesondere von Telekommunikationsbetreibern und -betreiberinnen, können die Eingriffsintensität von polizeilichen Abfragebefugnissen stark be-

Angelika Adensamer



Angelika Adensamer beschäftigt sich als Juristin und Kriminologin vor allem mit Kriminalpolitik, Überwachungsbefugnissen der Polizei und der Wahrung von Grundrechten in diesen Bereichen. Sie arbeitet bei der Grundrechts-NGO epicenter.works in Wien als Policy Advisor.

einflussen. So ist die österreichische Polizei befugt, ohne weitere Voraussetzungen Stammdaten von Telekommunikationsbetreibern und -betreiberinnen zu verlangen. Auch die Auskunft über Verkehrs- und Standortdaten ist unter bestimmten Voraussetzungen möglich. Üblicherweise speichern die Betreiber Verkehrs- und Standortdaten nur zu Verrechnungszwecken und löschen sie, sobald die Rechnungen unwidersprochen bezahlt wurden. Die Daten darüber hinaus zu speichern, ist nicht im Interesse der Anbieter und Anbieterinnen, sehr wohl aber in dem der Polizei, wie die nicht enden wollende Debatte um die Vorratsdatenspeicherung zeigt.

Mit der *Vorratsdatenspeicherung* sollte 2006 die EU-weite Verpflichtung geschaffen werden, die betreffenden Daten für sechs Monate zu speichern, um den Zugriff von Ermittlungsbehörden länger zu ermöglichen. Sie wurde vom EuGH jedoch 2014 für grundrechtswidrig erklärt. Dennoch gibt es auf EU-Ebene aktuell Bestrebungen, sie wieder einzuführen.[15] Hier wird eine Überwachungsmaßnahme nicht als polizeiliche Befugnis geregelt, sondern über den Umweg einer Speicherverpflichtung.

Mit dem Überwachungspaket wurde 2018 in Österreich unter anderem die *Anlassdatenspeicherung* (auch *Quick Freeze)* eingeführt. Nun können die Sicherheitsbehörden bei Bedarf eine Speicherpflicht von Verkehrs- Standort-, und Zugangsdaten von bis zu einem Jahr anordnen. Es handelt sich also quasi um eine – „Vorratsdatenspeicherung light".

Ähnlich ist es bei der *SIM-Karten-Registrierung,* welche in Österreich ebenfalls mit dem Überwachungspaket 2018 eingeführt wurde und seit 1.9.2019 in Kraft ist. Seither muss die Identität aller Personen registriert werden, die SIM-Karten oder Guthaben kaufen. Neu ist nicht nur eine Speicherverpflichtung sondern die Pflicht, die Käuferdaten überhaupt zu erheben.

Ermittlungstechnische Speicherverpflichtungen sind aber nicht die einzigen, die das Potenzial haben, Überwachung auszuweiten, ohne die gesetzlichen Grundlagen der Polizeiarbeit zu verändern. In dieser Hinsicht wurden beispielsweise Entwürfe zur Einführung einer *Digitalsteuer* der letzten österreichischen Bundesregierung kritisiert.[16] Eine Speicherverpflichtung von Browserhistorien zur Steuerberechnung würde dazu führen, dass die Sicherheitsbehörden auf diese Zugriff erlangen.

Eine Evaluierung von Überwachungsbefugnissen muss daher besonderes Augenmerk auf Auskunftsbefugnisse der Polizei legen und mit Erhebungen darüber einhergehen, welche und wie viele Daten von diesen Auskunftsbefugnissen betroffen sind. Verändern sich die privat gespeicherten Daten in Umfang und Qualität, verändert sich auch die Eingriffsintensität der polizeilichen Befugnisse. So kommen immer mehr Daten von vernetzten Geräten, dem *Internet of Things,* dazu, die alle Lebensbereiche der Menschen in noch nie dagewesener Kleinteiligkeit abdecken.

Fazit

Ich hoffe, anhand dieser Beispiele überzeugend demonstriert zu haben, dass die Ausweitung von staatlicher Überwachung nicht nur durch die Ausweitung der gesetzlichen Ermittlungsbefugnisse geschieht, sondern auch durch neue Technologien und den

Bei epicenter.works wird gebaut.

Ausbau privater Datenspeicher. Diese, sowie die Größe der Datenbanken, die automatischen Analysen unterzogen werden, müssen in der Evaluierung von Befugnissen eine Rolle spielen und unter Umständen zu ihrem Rückbau führen. Das bedeutet auch, dass es nicht genug ist, sich als kritische Öffentlichkeit mit Gesetzesvorhaben zu beschäftigen, sondern dass es auch gilt technische Entwicklungen im Auge zu behalten sowie Speicherverpflichtungen und -praktiken Privater, die oft nicht in polizeirechtlichen Regelungsmaterien geändert werden.

Anmerkungen

1 *https://epicenter.works/sites/default/files/heat_v1.2.pdf.*
2 *1 Bvr 256/08 vom 2. März 2010, Rz 218. Vgl. auch Bieker/Bremert/Hagendorff, Die Überwachungs-Gesamtrechnung, oder: Es kann nicht sein, was nicht sein darf, in Roßnagel et al. (Hrsg.) Die Fortentwicklung des Datenschutzes (2018).*
3 *Vgl. Erläuterungen zum Strafprozessänderungsgesetz 2018 (17 d. B.) XXVI. GP, S. 2, https://www.parlament.gv.at/PAKT/VHG/XXVI/I/I_00017/fname_682032.pdf.*
4 *Wimmer, Polizei startet im Dezember mit Gesichtserkennung, futurezone.at vom 18.4.2019, https://futurezone.at/netzpolitik/polizei-startet-im-dezember-mit-gesichtserkennung/400469524.*
5 *Vgl. Bundesministerium für Inneres, Anfragebeantwortung vom 25.9.2019, https://fragdenstaat.at/anfrage/gesichtserkennung/.*
6 *Bundesministerium für Inneres, Anfragebeantwortung vom 11.6.2019, https://fragdenstaat.at/anfrage/ankauf-einer-gesichtserkennungs-software-durch-das-bundeskriminalamt/.*
7 *Bundesministerium für Inneres, Anfragebeantwortung vom 22.8.2019, https://fragdenstaat.at/anfrage/drohneneinsatze-durch-die-polizei/.*
8 *Blees, Polizei testet Drohnen, Neues Deutschland vom 3.9.2019, https://www.neues-deutschland.de/artikel/1125253.berlin-polizei-testet-drohnen.html.*
9 *Bundesministerium für Inneres, Anfragebeantwortung vom 5.9.2019, https://fragdenstaat.at/anfrage/predictive-policing/.*
10 *Richtlinie (EU) 2016/681 des Europäischen Parlaments und des Rates vom 27. April 2016 über die Verwendung von Fluggastdatensätzen (PNR-Daten) zur Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität.*
11 *Allein in Deutschland wird von bis zu 180 Millionen betroffenen Personen pr Jahr ausgegangen (laut Anfrage der Abgeordneten Andrej Hunko, Martina Renner, Jan Korte u. a. http://dipbt.bundestag.de/doc/btd/19/095/1909536.pdf). In Österreich, mit einer Gesamtbevölkerung von ca. 8,5 Millionen, waren im nicht voll ausgebauten Betrieb in den ersten acht Monaten schon 11,9 Millionen Menschen betroffen*

(Bundesministerium für Inneres, Anfragebeantwortung vom 8.10.2019, https://fragdenstaat.at/anfrage/fluggastdatenanalyse-datenschutz-rechtliche-aspekte/).

12 *Zur ausführlichen Erklärung des Prävalenzfehlers und seiner Auswirkungen auf Systeme der Massenüberwachung sei McDermott, An Explainer On The Base Rate Fallacy empfohlen (https://en.epicenter.works/content/an-explainer-on-the-base-rate-fallacy-and-pnr).*

13 *Siehe die Zahlen des Bundesministerium für Inneres, Anfragebeantwortung vom 8.10.2019, https://fragdenstaat.at/anfrage/fluggastdatenanalyse-datenschutzrechtliche-aspekte/.*

14 *https://nopnr.eu/pnr/.*

15 *Vgl. z. B. Rat der EU, Vorratsdatenspeicherung zum Zweck der Kriminalitätsbekämpfung: Rat verabschiedet Schlussfolgerungen, https://www.consilium.europa.eu/de/press/press-releases/2019/06/06/data-retention-to-fight-crime-council-adopts-conclusions/.*

16 *Epicenter.works, Digitalsteuergesetz schreibt bis dato unerlaubte Datenspeicherung vor, Blogpost vom 9.5.2019, https://epicenter.works/content/digitalsteuergesetz-schreibt-bis-dato-unerlaubte-datenspeicherung-vor.*

David Leeuwestein

Die wundersame Kreativität der GesetzgeberInnen

Haben Sie sich schon einmal gefragt, was der Staat eigentlich alles über Sie weiß? Welche verschiedenen Behörden Daten über Sie erheben, verknüpfen und analysieren? Waren sie schon mal verärgert oder verunsichert darüber, dass Sie nicht mehr wissen, welchen digitalen Fingerabdruck sie bei einer Verkehrskontrolle hinterlassen, einer Flugreise, einem Website-Aufruf?

Vermeintliche SicherheitspolitikerInnen erlassen immer mehr Gesetze, um unser digitales und analoges Leben bestmöglich zu überwachen. Polizeigesetze, Vorratsdatenspeicherung und Staatstrojaner bilden nur die Spitze des Eisbergs. Schon längst ist es für Einzelne unmöglich geworden, zu überblicken wie genau sie oder er von wem unter welchen Umständen überwacht werden darf.

Das hat das Bundesverfassungsgericht bereits vor Jahren als Problem erkannt. In seinem Urteil zur Vorratsdatenspeicherung 2010 hielt das Gericht fest, dass eine Vorratsdatenspeicherung zwar nicht per se verfassungswidrig sei, die Überwachung im Kontext bereits bestehender Überwachungsgesetze jedoch ein für die Demokratie gefährliches Maß erreiche. Aus diesem Urteil entstand der Begriff der Überwachungs-Gesamtrechnung.

Wir von Digitalcourage sind überzeugt, dass das für eine Demokratie verträgliche Maß an Überwachung schon lange überschritten ist. Um das zu belegen, pflegen wir schon seit Längerem eine Materialsammlung *(https://digitalcourage.de/ueberwachungsgesamtrechnung)* für eine Überwachungs-Gesamtrechnung, in der wir möglichst alle entstehenden und verabschiedeten Überwachungsgesetze erfassen. Als Absolvent eines Freiwilligen Sozialen Jahres bei Digitalcourage gehörte es zu meinem Aufgabenbereich, diese Übersicht aktuell zu halten.

Kein gutes Jahr

Schon die Gesetze, die in diesem einen Jahr dazugekommen sind, schaden unserer Demokratie empfindlich. Das sind unter Anderem:

- Das *Zensusvorbereitungsgesetz,* das zur Folge hatte, dass sensible Informationen wie Name, Geschlechtsidentität, Familienstand oder Religionszugehörigkeit von allen BundesbürgerInnen im Rahmen eines Testlaufs für den Zensus 21 im Statistischen Bundesamt zentral zusammengeführt wurden – ohne sie vorher zu anonymisieren oder pseudonymisieren. Das Gesetz sieht eine maximale Aufbewahrungsfrist von bis zu zwei Jahren vor.

- Das *Neunte Gesetz zur Änderung des Straßenverkehrsgesetzes,* das Autofahrer mit Überwachung für den Dieselskandal straft, anstatt die Autokonzerne in die Verantwortung zu nehmen.

- Das *European Travel Information and Authorisation System (ETIAS),* welches vorschreibt, dass alle Menschen, die aus Nicht-EU-Staaten einreisen möchten, sofern sie kein Visum benötigen, eine Reisegenehmigung (ETIAS Genehmigung) einholen müssen. Die erhobenen Daten wie Alter, Geschlecht, Nationalität, Gesundheitszustand und vorherige Reisen sollen durch einen Algorithmus auf Risikoindikatoren untersucht und gegen diverse Datenbanken abgeglichen werden.

- Die Ausweitung der EU-weiten Fahndungsdatenbank *SIS II,* die vorgibt, dass bei allen Treffern, die im Zusammenhang mit Terrorismus stehen, ab Ende 2019 die Behörde Europol informiert werden muss. Zusätzlich können nun auch Ermittlungsanfragen gestellt werden. Diese legen Fragen oder Informationen fest, auf deren Grundlage die betroffene Person bei einer Polizeikontrolle befragt wird. Zudem wird der Eintrag von „Rückführentscheidungen abgelehnter AsylantragstellerInnen“ verpflichtend.

- Die *Verordnung zur Erhöhung der Sicherheit der Personalausweise von Unionsbürgern,* welche nahezu alle EU-BürgerInnen zur Abgabe von Fingerabdrücken zwingt. *(https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32019R1157)*

- Das Zentralisierte System für die Ermittlung der Mitgliedstaaten, in denen Informationen zu Verurteilungen von Drittstaatsangehörigen und Staatenlosen vorliegen *(ECRIS-TCN),* in dem biometrische Daten (Fingerabdrücke und Passbild) sowie biographische Informationen über alle in der

EU verurteilten StraftäterInnen aus dem Ausland gespeichert werden sollen.

- Das *Urheberrechtsschutzgesetz,* welches Uploadfilter und ein EU-weites Leistungsschutzrecht eingeführt hat. Es ist wahrscheinlich, dass DiensteanbieterInnen auf fertige Lösungen von Konzernen wie Google zurückgreifen werden, um Uploadfilter zu implementieren. Das wird deren ohnehin schon bedrückende Machtstellung weiter ausbauen.

- Zudem wurden zahlreiche Landes-*Polizeigesetze* verschärft. In allen Fällen bedeutet die Verschärfung einen massiven Grundrechteabbau und eine Gefährdung des Rechtsstaats. (Übersicht unter: *https://digitalcourage.de/blog/2018/uebersicht-polizeigesetze*). In Nordrhein-Westfalen führte das Polizeigesetz etwa die Schleierfahndung, mehr Videoüberwachung und Staatstrojaner ein.

Dies sind jedoch nur die Gesetze, die schon verabschiedet wurden und höchstens noch durch Klagen aufgehalten werden können. Zahlreiche weitere Gesetze befinden sich entweder gerade im Verabschiedungsprozess oder sind noch in der Abstimmungsphase.

Die nächsten Jahre werden nicht besser

Zu den geplanten Gesetzesprojekten zählen aktuell etwa:

- Eine Neuauflage der *EU-weiten Vorratsdatenspeicherung:* Bis zu 487 verschiedene Datenkategorien sollen nach dem aktuellen Plan auf Vorrat und verdachtsunabhängig von allen EU-BürgerInnen gespeichert werden. Das diskutiert der EU-Rat zur Zeit. Dazu zählen Standortdaten, Verbindungsdaten u. v. m. Auch Diensteanbieter (OTTs) wie *WhatsApp* sollen von der neuen Vorratsdatenspeicherung erfasst werden.

- Das *Verfassungsschutzgesetz:* Auch Verfassungsschutz und Bundesnachrichtendienst sollen Staatstrojaner einsetzen dürfen. Zudem soll das Mindestalter für Personen, die vom Verfassungsschutz beobachtet werden dürfen, ersatzlos gestrichen werden.

- Der Entwurf eines *Strafrechts-Änderungsgesetzes* – Einführung einer eigenständigen Strafbarkeit für das Betreiben von internetbasierten Handelsplattformen für illegale Waren und Dienstleistungen *(Tor-Verbot):* Der Bundesrat will einen neuen Straftatbestand gegen Betreiber sogenannter *Darknet-Märkte* einführen. Im schlimmsten Fall wird das Betreiben von Tor-Servern illegal.

- Das EU-Vorhaben *TERREG:* Alle Onlinedienste sollen verpflichtet werden, gemeldete Nutzerkommentare innerhalb von einer Stunde offline zu nehmen. Außerdem werden die Diensteanbieter dazu verpflichtet, proaktiv mithilfe von Künstlichen Neuronalen Netzwerken, Hash-Tabellen und Uploadfiltern terroristische Inhalte zu filtern.

- Die geplante *Interoperabilität von EU-Datenbanken:* Fünf große Biometrie-Datenbanken sollen in einem „gemeinsamen Identitätsspeicher" zusammengelegt werden. Dies betrifft die StraftäterInnen-Datenbank ECRIS-TCN, das Visa Information System, das Flüchtlingsregister EURODAC, die Reisedatenbank ETIAS und das noch geplante Entry Exit System (EES). Zudem sollen die Strafverfolgungsbehörden eine Suchmaske erhalten, um alle diese Datenbanken in einem Zug abfragen zu können.

- Der *Detektor für Mehrfachidentitäten:* Er soll die hinterlegten Fingerabdrücke und Gesichtsbilder in den fünf großen Biometrie-Datenbanken der EU (ECRIS-TCN, VIS, EURODAC, ETIAS und EES) durchsuchen und Menschen ausfindig machen, die unter verschiedenen Identitäten erfasst wurden. Das wird automatisch geschehen.

- Der *Eurotrojaner:* Medienberichten zufolge soll Europol mit einem „Eurotrojaner" getauften Staatstrojaner ausgestattet werden. Dieser soll sogar Zero-Day-Sicherheitslücken nutzen.

- Das EU-Vorhaben *Tensor:* Im Rahmen dieses Projekts forschen europäische Polizeibehörden und Rüstungsfirmen an Uploadfiltern, die auch unbekannte terroristische Inhalte erkennen und entfernen sollen. Die EU-Kommission hat dafür fünf Millionen Euro bereitgestellt.

- Der *Cloud-Act:* Polizei- und Justizbehörden sollen zukünftig leichter auf Cloud-Daten in den USA zugreifen. Umgekehrt könnten auch US-Behörden direkt bei europäischen Internetfirmen anklopfen.

- Das *zweite „Datenaustauschverbesserungsgesetz":* Das Mindestalter zur verpflichtenden Abnahme von Fingerabdrücken Geflüchteter soll von 14 auf sechs Jahre gesenkt werden. Zudem sollen lokale und Länderbehörden das Ausländerzentralregister mit eigenen Daten anreichen dürfen. Auch die Zugriffsbefugnisse für Behörden (insbesondere Sicherheitsbehörden) werden massiv ausgeweitet.

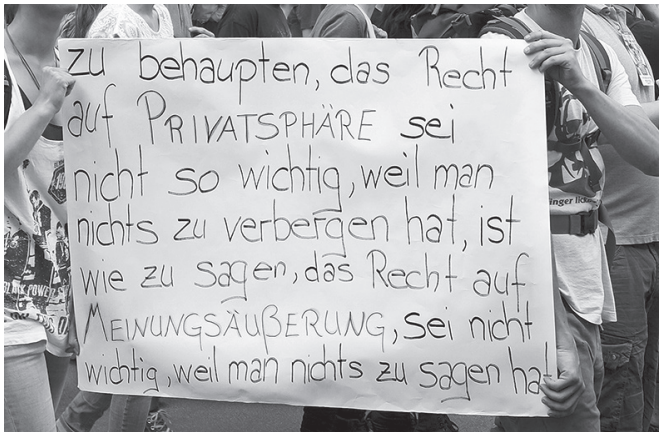
- Die *E-Evidence-Verordnung:* Betreiber von Internet-Diensten sollen Daten ihrer NutzerInnen künftig direkt und mitun-

David Leeuwestein

David Leeuwestein kommt aus einer Kleinstadt inmitten des digitalen Niemandslandes Brandenburg. Dennoch kam er früh mit den Themen Datenschutz, IT-Sicherheit und Hacking in Berührung. Sein Interesse für Politik lebte er zunächst in einer Lokalzeitung aus. Er unterstützte das Digitalcourage-Team 2018 und 2019 als Freiwilliger im FSJ.

ter innerhalb von sechs Stunden für Behörden aus allen EU-Ländern zugänglich machen. Andernfalls drohen Strafen von bis zu 2 % des Jahresumsatzes. Vorbild für das Gesetzesvorhaben ist der Cloud-Act in den USA.

Eine vollständige Übersicht unserer Sammlung finden Sie auf unserer Website: *https://digitalcourage.de/ueberwachungsgesamtrechnung/sammlung*. Wir freuen uns über Hinweise und Ergänzungen.



Das Recht auf Privatsphäre, Foto: Günther Gerstenberg

Wie die Erfahrung zeigt, werden Überwachungsgesetze gerne ergänzt und ausgebaut, jedoch fast nie zurückgenommen. Mittlerweile erreicht der Überwachungswahn ein Maß, das auch für eine kritische Öffentlichkeit nur noch schwer zu überblicken ist. Ohne die unermüdliche Arbeit von Journalistinnen, Politikern und Aktivistinnen wäre unsere Materialsammlung niemals zu ihrer jetzigen annähernden Vollständigkeit gelangt.

Doch nicht nur die Erfassung bekannter Überwachungsvorhaben ist eine immense Herausforderung, immer öfter liegt die Aufgabe auch darin, solche Vorhaben ausfindig zu machen.

Unserer Veröffentlichung interner Dokumente über eine Neuauflage der EU-weiten Vorratsdatenspeicherung ging etwa ein monatelanger Rechercheprozess voraus, in dem wir zahlreiche Dokumente von Behörden angefragt und ausgewertet haben. In der Vergangenheit waren diese Recherchen zudem immer von rechtlichen Auseinandersetzungen mit verschiedenen Behörden begleitet, da diese die Herausgabe entscheidender Dokumente verweigerten.

Auch vermeintliche Pro-Datenschutz-Gesetze entpuppen sich zunehmend als Kompetenzgeber für Datenkraken. So droht etwa die aktuell verhandelte E-Privacy-Verordnung zu einer Hintertür für eine private Vorratsdatenspeicherung zu werden: Diensteanbietern soll das Speichern möglichst attraktiv gemacht werden, sodass die freiwillig gespeicherten Daten lediglich noch nach bereits geltendem Recht angefragt werden müssen.

Was wir fordern

Dem bereits 2010 vom Bundesverfassungsgericht geforderten Prinzip der Überwachungs-Gesamtrechnung schenkt der Gesetzgeber dabei bis heute keine Beachtung. Somit fehlt der Öffentlichkeit ein entscheidendes Werkzeug, um neue Überwachungsgesetze bewerten zu können. Sie weiß schlicht nicht mehr, wie sie sich ins Gesamtmaß staatlicher Eingriffe einfügen. Besondere Risikogruppen wie AnwältInnen, Journalisten oder AktivistInnen fallen in dem Diskurs sowieso unter den Tisch.

Wir fordern daher, dass der Gesetzgeber sich endlich an die bereits seit 2010 bestehenden Vorgaben des Bundesverfassungsgerichts hält und bei jedem neuen Überwachungsgesetz

1. eine Auflistung aller bestehenden Überwachungsgesetze vorlegt, und

2. begründet, warum dieses neue Vorhaben dennoch zielführend, notwendig und verhältnismäßig ist.

Und wir fordern echte Sicherheitspolitik statt Überwachung: Investieren in Gesundheit, Bildung, Wohnraum und soziale Sicherheit. Es darf nicht sein, dass vermeintliche SicherheitspolitikerInnen mit euphemistischen Gesetzesnamen oder mit kurzfristigen Änderungsanträgen der Bevölkerung Überwachungsmaßnahmen unterschieben. Das für eine Demokratie kritische Maß an Überwachung ist schon lange erreicht.

Frank Herrmann

Denn sie wissen nicht, was sie tun. Oder doch?

Es liegt im Wesen der Überwachung, dass sie für sehr lange Zeit weit weg, ja unsichtbar bleibt, jedoch ganz plötzlich wahrgenommen wird, wenn sich eine persönliche Betroffenheit einstellt. Und es liegt im Wesen der Politik, vor allem der Regierungspolitik, dass für aktuelle Probleme meist die schnelle Aufmerksamkeit und kurzfristige Lösungsversprechen im Vordergrund stehen, denn die nächste Wahl steht immer irgendwo vor der Tür.

Nicht die besten Voraussetzungen für ein Parlament, im täglichen Politikbetrieb auch die noch nicht offensichtlichen Auswirkungen beschlossener Gesetze wahrzunehmen und bei der weiteren Gesetzgebung zu berücksichtigen. Doch genau das wäre die Aufgabe, zu der das Bundesverfassungsgericht den Gesetzgeber verpflichtet. Es verlangt von ihm den „Blick auf die Gesamtheit der verschiedenen schon vorhandenen Datensammlungen“[1], wenn er weitere Datenspeicherungspflichten plant, also die Betrachtung in einer Überwachungs-Gesamtrechnung. Aber wer soll diese aufstellen? Und wer hat überhaupt ein Interesse daran?

Das Parlament macht die Regeln

Im demokratischen Rechtsstaat kommt der gesetzgebenden Gewalt, in Deutschland also dem Bundestag und den Landtagen, eine zentrale Aufgabe zu: Hier werden die Regeln beschlossen, nach denen wir zusammenleben, und es werden die Grenzen bestimmt, was Sicherheitsbehörden dürfen oder eben nicht. Die dort verhandelten Gesetze regeln auch die Aufgaben und den Handlungsrahmen der Regierungen und sie bilden die Basis, auf der Gerichte im Streitfall die Rechtslage verbindlich klären.

Im Idealfall würde sich also ein Parlament in der Gesamtheit seiner den Menschen im Land verpflichteten Abgeordneten um den Schutz und die Wahrung der Grundrechte kümmern.

> *„Das Anstellen einer sog. Überwachungsgesamtrechnung [ist insoweit] verfassungsrechtliche, parlamentarische Pflicht; jedenfalls bei Gesetzesvorhaben, die die Schaffung neuer vorsorglicher, anlassloser Datensammlungen zum Gegenstand haben. Nur in wertender Einbeziehung bereits bestehender Datensammlungen kann dann die Verhältnismäßigkeit neuer Erhebungs- und Speicherungsbefugnisse überprüft werden."*[2]

Die Praxis sieht allerdings vielfach anders aus. Zwar wird in parlamentarischen Reden immer wieder „die Bedeutung des hohen Hauses" herausgestellt und dass man sich „eingehend mit einem zur Abstimmung anstehenden Gesetzesvorhaben befasst habe", aber solche Aussagen der Abgeordneten sind schwer zu prüfen.

Erschwerend kommt hinzu, das Abgeordnete selten für sich allein, sondern meist für ihre Fraktion sprechen. Die Menge der Stimmen mit möglicherweise unterschiedlichen Ansichten zur debattierten Problemlage schrumpft dann schnell auf die Handvoll im jeweiligen Parlament vertretenen Fraktionen zusammen. Und auch wenn am Ende der Beratungen, zur Abstimmung, immer nur noch zwei unterschiedliche Stimmen vorhanden sind, ja und nein, dann ist dieses Abstimmverhalten in fast allen Fällen schon von Beginn an festgelegt, völlig unabhängig vom Thema. Denn die Parteien, die alleine, bzw. aktuell meist in Koalitionen, die Regierung bilden, haben auch im Parlament mit ihren Fraktionen die Mehrheit. Sie sind die „regierungstragenden Fraktionen".

Das Handlungs-Paradox des Parlaments

Wenn die Regierung dem Parlament einen Gesetzentwurf beispielsweise über den in ihren Augen notwendigen Einsatz der Funkzellenüberwachung auch zur Aufklärung von Taschendiebstählen vorlegt, dann würde dieser mit der Mehrheit der regierungstragenden Fraktionen in aller Regel auch angenommen. Die Ablehnung eines Gesetzes, das von der eigenen Regierung eingebracht wurde, käme einem Misstrauensvotum gleich.

> *„Festzuhalten ist, dass sich das Parlament bei Einführung anlassloser Datensammlungen stets der Prüfung zu stellen hat, ob die betreffende staatliche Aufgabe auch durch (bestehende) ‚anlassbezogenere' Datenverarbeitungsmaßnahmen bewerkstelligt werden kann. Damit die Volksvertretungen dies beurteilen können, bedarf es einer Evaluierung aller größeren staatlichen Datensammlungen in den jeweiligen Sicherheitsbereichen", vermerkt Prof. Dr. Frank Braun in einer Stellungnahme für den Landtag NRW.*[3]

Da eine derartige Überwachungs-Gesamtrechnung dazu geeignet wäre, den Beschluss des von der Regierung eingebrachten Gesetzentwurfs möglicherweise zu verzögern oder gar zu verhindern, wird die Parlamentsmehrheit nach heutiger Praxis eine solche Evaluation nicht durchführen. Die eigentliche Aufgabe des Parlaments, nämlich die Regierung zu kontrollieren, findet so nicht statt.

Die Regierung wird beauftragt

Neben Gesetzen werden im Parlament auch sogenannte Anträge beschlossen. Dabei handelt es sich meist um Absichtserklärungen, aber auch um Handlungsanweisungen und Arbeitsaufträge an die jeweilige Regierung. Anträge werden üblicherweise von der Opposition gestellt und üblicherweise von der Mehrheit der regierungstragenden Fraktionen abgelehnt. Anträge sind jedoch im aktuellen parlamentarischen System das einzige Mittel, um durch die öffentliche Debatte im Parlament auf Missstände oder Versäumnisse der Regierung hinzuweisen oder die Beachtung bzw. Umsetzung höchstrichterlicher Urteile anzumahnen.

Zur Erstellung einer Überwachungs-Gesamtrechnung hat es seit der Urteilsverkündung des Bundesverfassungsgerichts (BVerfG) im Jahr 2010 ganze drei Anträge in deutschen Parlamenten gegeben. Aufgestellt wurde eine Überwachungs-Gesamtrechnung bis heute nicht.

Im April 2019 stellte die Fraktion Bündnis 90/Die Grünen im bayrischen Landtag den Antrag „Unabhängiges Forschungsprojekt zum neuen Polizeiaufgabengesetz"[4] und forderte darin

> *„die Staatsregierung [auf], ein unabhängiges wissenschaftliches Institut mit einem rechtstatsächlichen Forschungsprojekt [...] zu beauftragen und dem Landtag über die Ergebnisse des Forschungsprojekts zu berichten. Das Forschungsprojekt soll insbesondere auch eine ‚Überwachungsgesamtrechnung für Bayern' erstellen und bewerten."*

Der Antrag wurde nach Vorstellung im zuständigen Fachausschuss ohne weitere Beratung abgelehnt[5].

Der Antrag *Smart Germany – Digitalisierung und Bürgerrechte*[6] wurde im Oktober 2019 durch die FDP-Fraktion in den Deutschen Bundestag eingebracht und befindet sich aktuell noch im parlamentarischen Verfahren. Der Antrag „fordert die Bundesregierung auf, im Rahmen jedes Gesetzesvorhabens, durch welches neue Überwachungsbefugnisse eingeführt werden sollen – wie vom Bundesverfassungsgericht vorgesehen – eine Überwachungsgesamtrechnung durchzuführen [...]".

Beide genannten Anträge fordern von den Regierungen jeweils einen fertigen Bericht und nehmen damit dem Parlament die Möglichkeit, eigene Analysen und Bewertungen vorzunehmen.

Auch wenn die Grünen im bayrischen Landtag ein „unabhängiges wissenschaftliches Institut“ beauftragt sehen wollten, so wären die Kriterien zur Aufstellung einer Überwachungs-Gesamtrechnung doch von der Landesregierung festgelegt worden.

Und wie sich die Sichtweise der Regierungen darstellt, ist aus einer Anfrage der Fraktion Bündnis 90/Die Grünen vom April 2019[7] an die Bundesregierung abzulesen. Auf die Frage: „Welche Maßnahmen, Vorschläge und/oder politischen Prozesse hat die Bundesregierung bislang angestoßen oder plant sie aufzunehmen, um der […] ‚Notwendigkeit, alle staatlichen Überwachungsmöglichkeiten auf ein Maß zu beschränken, bei dem die Freiheitswahrnehmung der Bürger nicht total erfasst und registriert wird', gerecht zu werden […]?“ folgt die Antwort: „Nach Ansicht der Bundesregierung wird durch Rechtsordnung und Verwaltungsvollzug gewährleistet, dass ‚die Freiheitswahrnehmung der Bürger nicht total erfasst und registriert' wird.“

Eine Antwort, die zeigt, dass weder die Konzeption noch die Interpretation einer Überwachungs-Gesamtrechnung allein den Regierungsstellen überlassen werden sollte.

Foto: privat

Das Parlament muss es machen

Der dritte Antrag, *Überwachungsgesamtrechnung vorlegen: Transparenz über Situation der Freiheiten in unserer Gesellschaft schaffen!*[8], wurde von der Fraktion der PIRATEN bereits im Juni 2015 in den Landtag Nordrhein-Westfalen eingebracht. Darin wurde die Landesregierung u. a. aufgefordert,

> *„dem Landtag einen Bericht über die bestehenden staatlichen oder staatlich beauftragten Datensammlungen (‚Überwachungsgesamtrechnung') vorzulegen, die mindestens die folgenden Aspekte umfasst:*
>
> *a. Stand der bestehenden Überwachungsmaßnahmen durch die Behörden des Landes Nordrhein-Westfalen*
>
> *b. Überblick über die die Bürgerinnen und Bürger Nordrhein-Westfalens betreffenden bestehenden Datensammlungen durch Bundes- und EU-Behörden*
>
> *c. Stand der wissenschaftlichen Erkenntnisse zur Auswertbarkeit von Metadaten, pseudonymisierten und anonymisierten Daten*
>
> *[sowie] eine unabhängige Forschungsarbeit in Auftrag zu geben, die die Erarbeitung wissenschaftlich fundierter Kriterien zur Auswertung bestehender Datensammlungen im Sinne einer doppelten Verhältnismäßigkeitsprüfung sowie eine empirische Analyse der gegebenen Überwachungsgesamtrechnung umfasst.“*

Mit diesen Daten wäre der Landtag Nordrhein-Westfalen selbst in die Lage versetzt worden, eigene Bewertungen anzustellen, ob die bei neuen Gesetzesvorhaben beabsichtigten Grundrechtseingriffe wirklich notwendig sind. Auch dieser Antrag einer Oppositionspartei ist von der Regierungsmehrheit im Landtag abgelehnt worden. Allerdings hat auf Antrag der Fraktion der PIRATEN vorher noch eine Anhörung von Sachverständigen stattgefunden, und die liefert wertvolle Argumente für aktuelle und zukünftige Forderungen, endlich eine Gesamtbetrachtung der verbliebenen Freiräume der Gesellschaft in der immer weiter digital erfassten und ausgewerteten Welt aufzustellen.

Es reicht eben nicht, wieder auf das Bundesverfassungsgericht zu warten[9], bis bereits beschlossene und in der Anwendung befindliche Überwachungs-Gesetze höchstrichterlich korrigiert oder für nichtig erklärt werden. Werden vorliegende Urteile von den Verantwortlichen nicht befolgt und umgesetzt, dann stellt das das Rechtsstaatsprinzip insgesamt in Frage!

Die Sachverständigen in der oben genannten Anhörung im Landtag Nordrhein-Westfalen haben sich daher auch klar positioniert und beschrieben, was zu tun ist.

Als Verantwortlicher für die Umsetzung der Überwachungs-Gesamtrechnung wird vom Bundesverfassungsgericht der Gesetzgeber benannt, also die Landtage und der Bundestag. Der Sachverständige Rechtsanwalt Meinhard Starostik[10] erläuterte die Situation im Landesrecht so:

> *„Insofern ist der Gesetzgeber des Landes Nordrhein-Westfalen gehalten, die Grundrechte der Bürger des Bundeslandes so zu schützen wie der Bundesgesetzgeber auf Bundesebene. Gerade wegen der gesetzlichen Gestaltungsmöglichkeiten die der Landesgesetzgeber im Bereich des Polizeirechts hat, ist er auch verpflichtet, die Auswirkungen seiner gesetzgeberischen Anordnungen zu überprüfen bzw. zu erwägen.*
>
> *In solchen Überlegungen sind nicht nur die gesetzgeberischen Anordnungen, sondern auch die tatsächlichen Auswirkungen bereits vorhandener Überwachungsmaßnahmen zu berücksichtigen. Durch die Digitalisierung praktisch aller Bereiche der Technik, die mit Überwachung zu tun haben, ist eine qualitative Veränderung der Überwachungsmöglichkeiten eingetreten. Kameraüberwachungen sind präziser geworden, praktisch jede Funkzellenüberwachung führt zur Erhebung von zig-tausenden von Daten, die Kombination von Daten aus einer einzelnen Sammlung mit den Daten anderer Sammlungen, zum Beispiel durch Zusammenführung*

von Daten, die auf Landesebene erhoben wurden mit denen anderer Bundesländer und von Bundesbehörden, führen zu einer neuen Qualität der Überwachung."

Gerade im Hinblick auf die in den letzten Monaten vorgenommenen Änderungen der Polizeigesetze in vielen Bundesländern ist festzustellen, das nirgendwo ein Parlament seiner Verantwortung nachgekommen ist und eine Gesamtschau der bereits bestehenden Maßnahmen erstellt hat! Auch die Ausweitung oder auch Neueinführung statistischer Berichtspflichten über die bisherige Anwendung von Überwachungsmaßnahmen wurde bei den Gesetzesänderungen nicht berücksichtigt.

Dazu schreibt der Sachverständige Prof. Dr. Alexander Roßnagel in seinem Gutachten[11]:

„Aus der Schutzpflicht für die Freiheit der Bürger vor einem nicht mehr vertretbaren Grad an Überwachung ergibt sich für den Gesetzgeber eine Pflicht zur kontinuierlichen Beobachtung des Grads gesamtgesellschaftlicher Überwachung. [...]

Damit die Gesetzgeber und die Regierungen ihre Beobachtungs- und Abwägungspflicht erfüllen können, benötigen sie ausreichendes Wissen über den jeweils erreichten Stand staatlicher Überwachungsmöglichkeiten. Daher ist es notwendig, Regelungen für das Gewinnen und Aufbereiten des notwendigen Wissens zu treffen.

Zur Durchführung einer Überwachungs-Gesamtrechnung ist es erforderlich, das dafür benötigte Datenmaterial verfügbar zu halten. Insofern bestehen zum einen Beobachtungspflichten zur Praxis der staatlichen Überwachung. Hier ist ein erster Schritt, eine zentrale Statistik über alle Einsätze der Überwachungsinstrumente aufzubauen. Um eine qualitative Bewertung zu ermöglichen, ist es auch erforderlich, eine Erfolgskontrolle über die Verwendung der erhobenen Daten und den Ausgang der jeweiligen Verfahren und Maßnahmen zu haben."

Die statistische Erfassung der Einsätze von Überwachungsinstrumenten sollte landesweit schon lange eine Selbstverständlichkeit sein. Tatsächlich werden aber bis heute viel zu wenig Daten über die Nutzung der Befugnisse erfasst.

Bereiche, in denen sehr viele Daten entstehen und die Nutzung von Services intensiv (durch die Anbieter) ausgewertet wird, sind Internet, Social Media und E-Commerce. Auch wenn es hier nicht staatliche Stellen sind, sondern die Privatwirtschaft mit vielfach weltweit agierenden Konzernen, so können doch die jeweils lokalen Behörden auf die Daten zugreifen und internationale Kooperationsvereinbarungen im Kampf gegen den Terror haben Datenaustauschverfahren zwischen Sicherheitsbehörden weltweit geschaffen, die noch vor Jahren undenkbar waren. Prof. Dr. Alexander Roßnagel hat diesen Aspekt bereits in seiner Stellungnahme berücksichtigt und bezieht die Daten privater Unternehmen in das Budget der Überwachungs-Gesamtrechnung mit ein:

„Hinsichtlich der Pflicht, alle staatlichen Überwachungsmöglichkeiten auf ein Maß zu beschränken, bei dem die Freiheitswahrnehmung der Bürger nicht total erfasst und registriert wird, muss auch berücksichtigt werden, welche Informationen durch private Unternehmen gespeichert werden, etwa wie umfangreich die Erstellung von Personenprofilen oder wie hoch die Dichte privater Video-Überwachung ist. Denn diese Informationen stehen, soweit die entsprechenden Voraussetzungen vorliegen, staatlichen Stellen ebenfalls zur Verfügung."[12]

Denn sie wissen nicht, was sie tun, und das muss sich ändern!

Der riesige Umfang der zur Verfügung stehenden personenbezogenen Daten und die immer weiter perfektionierten Möglichkeiten, Massendaten zu analysieren und auszuwerten, stehen in krassem Gegensatz zu den Kenntnissen über die Häufigkeit der Anwendung dieser Möglichkeiten durch die Sicherheitsbehörden.

Die Abgeordneten wären in ihrer Gesamtheit gefordert, hier einen Anfang zu machen und für Transparenz zu sorgen. Tatsächlich verheddern sie sich in parteipolitischen Machtspielen. Doch wenn die Parlamente die vom Verfassungsgericht gestellte Auf-

Frank Herrmann

Frank Herrmann ist Berater für Datenschutz und Datenschutzbeauftragter für öffentliche und private Stellen. Bis 2009 war er parteilos politisch aktiv in der Anti-AKW-Bewegung und noch mehr im *AK Vorratsdatenspeicherung*, seit die EU-Richtlinie 2006/24/EG zur Vorratsdatenspeicherung verabschiedet wurde. Er ist einer der Beschwerdeführer vor dem Bundesverfassungsgericht gegen ihre deutsche Umsetzung. Seit 2009 ist er Mitglied der *Piratenpartei*, für die er von Mai 2012 bis Mai 2017 im Landtag von NRW saß. Er organisiert seit 2011 die *Freedom Not Fear* Konferenzen in Brüssel mit. Seit Oktober 2018 ist er 1. Vorsitzender des Landesverbandes NRW der Piratenpartei.

Seine Meinung: Wer Sicherheit der Freiheit vorzieht, der ist zu Recht ein Sklave (meint auch Aristoteles). Es ist nicht zu spät, für den Schutz der Privatheit in der digitalen Welt einzutreten. Jemand muss das machen!

gabe zum Schutz der Freiheit unserer Gemeinschaft nicht annehmen, dann ist das gleichbedeutend mit einer Bankrotterklärung der Volksvertretungen.

Rechtsanwalt Meinhard Starostik hatte zur Lösung des Problems einen interessanten Ansatz gebracht:

> *„Da die Überwachungspflicht den Gesetzgeber trifft, sollte meines Erachtens auch ein Ausschuss des Landtages federführend bei der Untersuchung seien. Dieser Ausschuss kann und sollte sowohl die zuständigen Fachbehörden (insbesondere Polizei und Verfassungsschutz) als auch die in dem jeweiligen Bereich sachkundigen Verbände, NGOs und Vertreter der Wissenschaft mit deren Sachverstand heranziehen."*[13]

Ein Grundrechte-Ausschuss, angesiedelt beim Landtag, aber unter Einbeziehung der Zivilgesellschaft, wäre einen Versuch wert. Denn wir brauchen dringend eine gesellschaftliche Debatte zu Überwachung und Freiheit in der digitalisierten Welt. Und wir brauchen eine Überwachungs-Gesamtrechnung als Grundlage für die Diskussion!

Anmerkungen

1 *BVerfG – 1 BvR 256/08 -, Rn. (218) https://www.bverfg.de/e/rs20100302_1bvr025608.html*
2 *MMST16-4197, S.12, https://www.landtag.nrw.de/portal/WWW/dokumentenarchiv/Dokument/MMST16-4197.pdf*
3 *MMST16-4197, S. 9, https://www.landtag.nrw.de/portal/WWW/dokumentenarchiv/Dokument/MMST16-4197.pdf*
4 *Drucksache Nr. 18/1535 vom 4.4.2019 https://www1.bayern.landtag.de/www/ElanTextAblage_WP18/Drucksachen/Basisdrucksachen/0000001000/0000001331.pdf*
5 *Beschlussempfehlung mit Bericht 18/2862 https://www.bayern.landtag.de/ElanTextAblage_WP18/Drucksachen/Folgedrucksachen/0000001000/0000001215.pdf*
6 *BT Drs. 1914058, https://dipbt.bundestag.de/dip21/btd/19/140/1914058.pdf*
7 *BT Drs. 1909705, Frage und Antwort Nr. 20, https://dipbt.bundestag.de/dip21/btd/19/097/1909705.pdf*
8 *MMD16-8976, https://www.landtag.nrw.de/portal/WWW/dokumentenarchiv/Dokument/MMD16-8976.pdf*
9 *Eine Übersicht über laufende Verfahren vor dem BVerfG ist hier abrufbar: https://www.bundesverfassungsgericht.de/DE/Verfahren/Jahresvorausschau/vs_2019/vorausschau_2019_node.html*
10 *MMST16-4214, https://www.landtag.nrw.de/portal/WWW/dokumentenarchiv/Dokument/MMST16-4214.pdf*
11 *MMST16-4232, S. 3, https://www.landtag.nrw.de/portal/WWW/dokumentenarchiv/Dokument/MMST16-4232.pdf*
12 *MMST16-4232, S. 2, https://www.landtag.nrw.de/portal/WWW/dokumentenarchiv/Dokument/MMST16-4232.pdf*
13 *MMST16-4214, S. 3, https://www.landtag.nrw.de/portal/WWW/dokumentenarchiv/Dokument/MMST16-4214.pdf*

Felix Bieker und Benjamin Bremert

Rote Linien im Sand, bei Sturm: Die Überwachungs-Gesamtrechnung[1]

Wenn es um die Schaffung oder Erweiterung staatlicher Überwachungsmaßnahmen geht, treibt den Gesetzgeber in jüngster Vergangenheit anscheinend nicht die Frage, wie viel Überwachung eine freiheitliche Gesellschaft notwendigerweise aushalten muss. Treibend scheint eher die Fragestellung zu sein, wie viel Freiheit man sich überhaupt noch erlauben könne. So werden in der politischen Debatte, etwa nach Anschlägen, reflexartig Vorratsdatenspeicherung oder andere Überwachungsmaßnahmen gefordert, ohne sich mit den Taten und den ihnen zugrundeliegenden Strukturen auseinanderzusetzen. Die Forderungen nach strengeren Überwachungsmaßnahmen können aber die strukturellen Probleme nicht lösen. Dazu kommt ein weiteres Problem, das zu adressieren ist: immer neue Überwachungsmaßnahmen haben auch Implikationen über ihren konkreten Anwendungsbereich hinaus.

Wenn es um staatliche Eingriffe in die Rechte der BürgerInnen geht, wird grundsätzlich nur der konkrete Eingriff betrachtet, um zu beurteilen, ob die Maßnahme rechtmäßig war. Anders verhält es sich – so jedenfalls die Theorie – im Kontext von Eingriffen durch Datenverarbeitung bei der Schaffung staatlicher Überwachungsmaßnahmen. Das Bundesverfassungsgericht (BVerfG) stellte schon im Volkszählungsurteil fest, dass „der Einzelne unter den Bedingungen einer automatischen Erhebung und Verarbeitung der seine Person betreffenden Angaben nicht zum bloßen Informationsobjekt" werden darf.[2] Im Jahr 2010 zog es daraus die Konsequenz, dass „die Freiheitswahrnehmung der Bürger nicht total erfasst und registriert werden darf".[3]

Im Angesicht der in diesem Verfahren verhandelten Vorratsdatenspeicherung sprang das Gericht aber recht kurz, als es dem Gesetzgeber diese Massenüberwachungsmaßnahme noch erlaubte, ihn aber zukünftig „zu größerer Zurückhaltung" gezwungen sah.[4] Dies verankerte das BVerfG auch gleich noch in der Verfassungsidentität des Grundgesetzes, um eine Vorlage zum vermeintlich grundrechtsmüden Gerichtshof der Europäischen Union (EuGH) umgehen zu können. Der EuGH überholte das BVerfG daraufhin bekanntlich mit seiner klaren Linie gegen die Vorratsdatenspeicherung,[5] die noch immer nachwirkt.[6]

Die Überwachungs-Gesamtrechnung und ihre unerwünschten Implikationen

Aus dem geschilderten Vabanquespiel des BVerfG zum Verbot einer Totalüberwachung leiteten findige Juristen eine Pflicht des Gesetzgebers ab, dass im Rahmen der Verhältnismäßigkeitsprüfung nun geprüft werden müsse, ob weitere Überwachungsgesetze diese vom BVerfG beschriebene Höchstgrenze überschrei-

ten – die Überwachungs-Gesamtrechnung erblickte das Licht der Welt.[7] Vor dem Hintergrund der vom BVerfG aufgestellten Grundsätze müssten bei der Beurteilung der Rechtmäßigkeit neuer Überwachungsmaßnahmen bestehende Maßnahmen und ihre konkrete Umsetzung bzw. praktische Anwendung berücksichtigt werden. Maßstab der Prüfung müsse neben dem konkreten Eingriff aufgrund der betreffenden Rechtsgrundlage auch der *kumulative Gesamtgrundrechtseingriff*[8] aller möglichen Überwachungsgesetze sein.[9]

Seit dem Urteil sind neun Jahre samt zahlreicher weiterer Überwachungsgesetze vergangen. Genannt seien hier nur die Quellen-TKÜ[10] und Online-Durchsuchung[11], die anlasslose Vorratsdatenspeicherung von Fluggastdaten[12] und die Regelungen zur Ausspähung des weltweiten Internetverkehrs.[13,14] Der Bundestag hat im Jahr 2016 eine Übersicht über verabschiedete Überwachungsgesetze erstellen lassen.[15] Diese enthielt eine kurze Zusammenfassung der entsprechenden Gesetze, eine Bewertung der durch sie erfolgenden Grundrechtseingriffe erfolgte jedoch nicht.

Der Gesetzgeber ignoriert die Überwachungs-Gesamtrechnung bisher also. Allerdings stehen ihrer Durchführung auch gewichtige praktische Probleme gegenüber.[16] Welche Gesetze müssen in die Betrachtung einfließen, wenn Überwachungsmaßnahmen auf EU-, Bundes-, Landesebene und teilweise von Kommunen beschlossen werden? Müssen regionale Unterschiede bei der Anwendung von Rechtsgrundlagen berücksichtigt werden und wie kann das adäquat geschehen? Was passiert, wenn das Höchstmaß überschritten wird: ist dann das erste oder letzte Überwachungsgesetz aufzuheben?[17] Wie können die einzelnen Grundrechtseingriffe untereinander in Bezug gesetzt und qualifiziert werden? Kann, unabhängig von politischen Erwägungen, ein objektiver Maßstab für ein Höchstmaß an Überwachung tatsächlich gebildet werden und auf welcher Grundlage hat das zu erfolgen? Und wird ein Gesetzgeber, dessen Überwachungsgesetze regelmäßig vom BVerfG geprüft und in Teilen verworfen werden, tatsächlich von sich aus zu der Einsicht gelangen, dass das Höchstmaß an Überwachung überschritten ist, wenn politisch ein stetiges Mehr an Überwachung gewollt ist?

Das größte Gewicht muss jedoch der Frage zukommen, was durch eine solche Überwachungs-Gesamtrechnung bewirkt wird: Das BVerfG zieht in einem Sturm aus Überwachungsmaßnahmen eine rote Linie in den Sand, die der Gesetzgeber nicht überschreiten darf, da er sonst einen Überwachungsstaat schaffe. Dabei wird angesichts der Vielzahl an bestehenden Überwachungsgesetzen die Prämisse, dass wir noch nicht in einer Überwachungsgesellschaft leben, wahrscheinlich nur noch in der Rechtswissenschaft ernsthaft vorgetragen.[18] Mit dieser Prämisse legitimiert aber das Gericht, das zum Schutz der Verfassung und damit der Grundrechte berufen ist, den Status quo und bescheinigt dem Gesetzgeber pauschal, dass das bisherige Ausmaß der Überwachung insgesamt nicht die Verfassung verletzt, obwohl es nur zur Beurteilung eines konkreten Überwachungsgesetzes angerufen war.

Gesetzes-DSFA als sinnvolle Alternative

Statt die Überwachungs-Gesamtrechnung mitsamt ihrer fatalen Legitimationswirkung weiter zu verfolgen, lohnt es sich also sinnvolle Alternativen zu finden, mit denen sich die Risiken von Überwachungsmaßnahmen identifizieren und beurteilen lassen. Eine Möglichkeit wäre, eine umfassendere Berücksichtigung des Gesamtsystems an Überwachungsgesetzen bereits im Gesetzgebungsverfahren zu verankern. So könnte der Gesetzgeber zur Durchführung einer Gesetzes-Datenschutz-Folgenabschätzung (Gesetzes-DSFA), wie sie in Art. 35 Abs. 10 DSGVO vorgesehen ist, verpflichtet werden und müsste danach schon im Stadium des Entwurfs neuer staatlicher Überwachungsmaßnahmen etwaige Auswirkungen, auch im Zusammenspiel mit anderen Maßnahmen, untersuchen und berücksichtigen.

Dadurch würde einerseits verhindert werden, dass unzulässige Gesetze überhaupt erst in Kraft treten und andererseits würde die notwendigerweise umfassende und daher zeitintensive Prüfung nicht mehr erstmalig im Wege eines gerichtlichen Verfahrens durchgeführt werden. Dabei ist jedoch zu beachten, dass es nicht bei einer Gesetzes-DSFA belassen werden darf, sondern auch eine reguläre DSFA erforderlich ist für die konkrete Umset-

Felix Bieker und Benjamin Bremert

Felix Bieker, LL.M. (Edinburgh) arbeitet seit 2013 im Projektreferat des *Unabhängigen Landeszentrums für Datenschutz (ULD)* und ist Mitglied im *Forum Privatheit*. Er beschäftigt sich mit Grundfragen des europäischen Grundrechts- und Datenschutzes, wie dem Begriff der Rechte und Freiheiten im EU-Datenschutzrecht. Daneben setzt er einen Fokus auf die Umsetzung datenschutzrechtlicher Verpflichtungen, wie der Ausgestaltung der Datenschutz-Folgenabschätzung. Er promoviert an der Universität Kiel zur individuellen und strukturellen Dimension des Grundrechts auf Datenschutz in der EU-Grundrechtecharta.

Benjamin Bremert arbeitet seit 2016 im Projektreferat des *Unabhängigen Landeszentrums für Datenschutz (ULD)* und ist Mitglied im *Forum Privatheit*. Er promoviert an der Universität Kiel zu Publizitätspflichten der Judikative.

zung der jeweiligen Maßnahme, die auf Grundlage eines Gesetzes ergeht.[19] Wenngleich dieser Ansatz nicht die *eine* Antwort auf alle inhaltlich aufgeworfenen Fragen bietet, so ist die Verankerung der umfassenden Prüfung im Gesetzgebungsverfahren systematisch naheliegender. Sie ermöglicht es dem Gesetzgeber, selbst Vorkehrungen zu treffen, wenn etwa die Intensität des damit verbundenen Grundrechtseingriffs zunächst der Umsetzung einer speziellen Maßnahme entgegensteht.

Fazit

Der aktuelle Rechtsstreit um die Vorratsdatenspeicherung ist inzwischen im Hauptsacheverfahren vor dem Bundesverwaltungsgericht angekommen. Dieses hat das Verfahren ausgesetzt, um dem EuGH Fragen zur Vereinbarkeit der deutschen Regelungen mit dem EU-Recht vorzulegen.[20] In der Zwischenzeit bleibt es bei der Nichtanwendung der Regelungen der Vorratsdatenspeicherung.

Unterdessen zeigt sich der Gesetzgeber von der roten Linie des BVerfG unbeeindruckt. Ein disziplinierender Effekt der Überwachungs-Gesamtrechnung ist augenscheinlich nicht eingetreten. Vielmehr zeigen die aufgeworfenen ungelösten und wohl unauflösbaren Fragen in Bezug auf die Überwachungs-Gesamtrechnung, dass diese kein geeignetes Instrument ist, um einer Totalerfassung der Freiheitswahrnehmungen der BürgerInnen entgegen zu wirken.

Für den Gesetzgeber ist es an der Zeit, mit einer Pflicht zur Durchführung einer Gesetzes-DSFA ein notwendiges Korrektiv in den Gesetzgebungsprozess einzubauen. Damit kann er gegenüber der Öffentlichkeit und den Gerichten demonstrieren, dass er die von ihm verlangte Abwägung verschiedener Positionen vornimmt. Mit der Gesetzes-DSFA ist es möglich, die Risiken von Überwachungsmaßnahmen für die betroffenen Individuen, aber auch den demokratisch verfassten Rechtsstaat, systematisch zu analysieren. Allerdings muss sichergestellt werden, dass auf die Durchführung einer notwendigerweise abstrakten Gesetzes-DSFA auch die Durchführung einer konkreten DSFA folgt. Nur eine solche konkrete DSFA kann die aufgrund einer Überwachungsmaßnahme umzusetzenden konkreten Verarbeitungsvorgänge und die sich daraus ergebenden konkreten Risiken für die Rechte und Freiheiten natürlicher Personen vollständig analysieren und durch geeignete Abhilfemaßnahmen eindämmen.

Foto: Günther Gerstenberg

Für das Bundesverfassungsgericht bleibt zu hoffen, dass es sich davon verabschiedet, rote Linien in den Sand zu malen, die der Gesetzgeber gewissenhaft bis über die Grenze ausfüllt, damit es sodann einige der überbordenden Rechtsgrundlagen wieder als verfassungswidrig verwerfen kann. Diesem Muster lässt sich aus Sicht der betroffenen Institutionen, Legislative und Judikative, womöglich sogar etwas abgewinnen: Es ermöglicht Bundestag und Bundesverfassungsgericht das Gesicht zu wahren. So können sie das Narrativ verbreiten, dass die jeweils vertretenen Positionen – Sicherheit auf der einen, Freiheit auf der anderen – durch das eigene Wirken befördert werden. Dieses Muster unterwandert jedoch die Grundrechte der Individuen, die alle Staatsgewalt zu schützen hat.

Anmerkungen

1 *Die Erstellung dieses Beitrags erfolgte im Rahmen des Forum Privatheit – Selbstbestimmtes Leben in der Digitalen Welt (https://www.forum-privatheit.de), das mit Mitteln des BMBF unter dem Förderkennzeichen 16KIS0747 gefördert wird.*

2 *BVerfG, Urteil vom 15.12.1983 – 1 BvR 209/83 u. a. = BVerfGE 65, 1 (43), Rn. 167 (Volkszählung).*

3 *BVerfG, Urteil vom 2.3.2010 – 1 BvR 256/08 u. a. = BVerfGE 125, 260, Rn. 218 (Vorratsdatenspeicherung).*

4 *Ebd.*

5 *EuGH, Urteil vom 8.4.2014, Rs. C-293/12 Digital Rights Ireland und Seitlinger u. a., ECLI:EU:C:2014:238.*

6 *EuGH, Urteil vom 21.12.2016, Rs. C-203/15 Tele2 Sverige, ECLI:EU:C:2016:970, Rn. 134; besprochen von Sandhu. Die Tele2-Entscheidung des EuGH zur Vorratsdatenspeicherung in den Mitgliedstaaten und ihre Auswirkungen auf die Rechtslage in Deutschland und in der Europäischen Union, EuR 2017, 453; vgl. auch die anhängigen Rs. C-623/17 Privacy International, Rs. C-520/18 Ordre des barreaux francophones et germanophone u. a. sowie verbunden Rs. C-511/18 und C-512/18 La Quadrature du Net u. a.*

7 *Roßnagel, Die „Überwachungs-Gesamtrechnung" – Das BVerfG und die Vorratsdatenspeicherung, NJW 2010, 1238.*

8 *Zu kumulativen bzw. additiven Grundrechtseingriffen etwa Voßkuhle/Kaiser, Grundwissen – Öffentliches Recht: Der Grundrechtseingriff, JuS 2009, 313, 314; Hornung, Die kumulative Wirkung von Überwachungsmaßnahmen: Eine Herausforderung an die Evaluierung von Sicherheitsgesetzen in: Albers/Weinzierl (Hrsg.), Menschenrechtliche Standards in der Sicherheitspolitik, Baden-Baden, 2010.*

9 *Roßnagel, a.a.O., S. 1240: Wonach eine „Gesamtbetrachtung des Stands staatlicher Überwachung" zu erfolgen habe.*

10 *Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens, BGBl. I 2017, 3202.*

11 *Ebd.*

12 *Gesetz zur Umsetzung der Richtlinie (EU) 2016/681, BGBl. I 2017, 1484.*

13 *Gesetz zur Ausland-Ausland-Fernmeldeaufklärung des Bundesnachrichtendienstes, BGBl. I 2016, 3346.*

14 *Eine hilfreiche Liste betreibt Digitalcourage e. V., abrufbar unter: https://digitalcourage.de/ueberwachungsgesamtrechnung/sammlung#staat.*

15 *Wissenschaftlicher Dienst des Deutschen Bundestags, Sachstand – Gesetzgebung zur Speicherung von personenbezogenen Daten, WD 3 – 3000 – 089/16 vom 15.3.2016.*

16 *Vgl. dazu ausführlich Bieker/Bremert/Hagendorff, Die Überwachungs-Gesamtrechnung, oder: Es kann nicht sein, was nicht sein darf, in: Roßnagel/Friedewald/Hansen (Hrsg.), Die Fortentwicklung des Datenschutzes, Wiesbaden, 2018.*

17 *So bereits Hornung/Schnabel, Das Urteil des Bundesverfassungsgerichts in Sachen Vorratsdatenspeicherung, DVBl. 2010, 824, 827.*

18 *Vgl. grundlegend schon Lyon, Surveillance society: monitoring everyday life, Buckingham, 2001; anschaulich auch Murakami Wood/Ball, A Report on the Surveillance Society, 2006, abrufbar unter: https://www.researchgate.net/publication/241917099_A_Report_on_the_Surveillance_Society.*

19 *Friedewald u. a., White Paper Datenschutz-Folgenabschätzung, 3. Aufl. 2017, abrufbar unter: https://www.forum-privatheit.de/wp-content/uploads/Forum-Privatheit-WP-DSFA-3-Auflage-2017-11-29.pdf.*

20 *BVerwG , Beschluss vom 25.09.2019 – 6 C 12.18; 6 C 13.18.*

Jörg Pohle*

Freiheitsbestandsanalyse statt Überwachungs-Gesamtrechnung

Ein Alternativvorschlag

Als das Bundesverfassungsgericht (BVerfG) im März 2010 die Vorratsdatenspeicherung für grundsätzlich mit dem Grundgesetz vereinbar, die konkrete Umsetzung im Telekommunikationsgesetz aber für verfassungswidrig und die entsprechenden Vorschriften für nichtig erklärte,[1] *schrieb es dem Gesetzgeber ins Stammbuch, er sei „bei der Erwägung neuer Speicherungspflichten oder -berechtigungen in Blick auf die Gesamtheit der verschiedenen schon vorhandenen Datensammlungen zu größerer Zurückhaltung"*[2] *gezwungen. Alexander Roßnagel hat das als Notwendigkeit zur doppelten Verhältnismäßigkeitsprüfung beschrieben: Neben die Bewertung der Verhältnismäßigkeit des Einsatzes eines Überwachungsinstruments auf der Grundlage seiner Wirkungen müsse eine Prüfung „auf der Basis einer Gesamtbetrachtung aller verfügbaren staatlichen Überwachungsmaßnahmen die Verhältnismäßigkeit der Gesamtbelastungen bürgerlicher Freiheiten" treten.*[3] *Für diese Gesamtbetrachtung prägte er dann den Terminus* Überwachungs-Gesamtrechnung[4] (ÜGR).

Überwachungs-Gesamtrechnung – Eine kritische Analyse

Der Begriff der Überwachungs-Gesamtrechnung verspricht mehr, als er halten kann. Eine ÜGR ist trotz ihres Namens weder eine *Überwachungs*-Gesamtrechnung noch eine Überwachungs-*Gesamt*rechnung noch eine Überwachungs-Gesamt-*rechnung*.

Meine Analyse wird sich auf einige ausgewählte Ansätze und Kritiken konzentrieren. An erster Stelle stehen dabei die Vorschläge von Roßnagel und seiner Arbeitsgruppe.[5] Der zweite zentrale Vorschlag wurde vom Arbeitskreis Vorratsdaten Österreich (AKVorrat), seit Ende 2016 epicenter.works, 2016 als *HEAT – Handbuch zur Evaluation der Anti-Terror-Gesetze* herausgegeben,[6] ein dritter von Tobias Starnecker in seiner Dissertation über Body-Cams und Dashcams 2017 als „modifizierte und konkretisierte Überwachungsgesamtrechnung".[7] Die umfassendste und zugleich wohl fundierteste Kritik an der ÜGR stammt aus der Feder von Felix Bieker, Benjamin Bremert und Thilo Hagendorff.[8]

Überwachungs…

Eine ÜGR geht über eine Analyse der kumulativen Wirkung von Eingriffen[9], „additiver Grundrechtseingriff"[10] genannt, hinaus und erweitert sie auf die gesellschaftliche Dimension staatlicher Überwachungstätigkeit.

Die Gruppe um Roßnagel sowie Starnecker legen ein traditionell liberales Verständnis von Überwachung als *staatlicher Überwachung* zu Zwecken von Gefahrenabwehr und Strafverfolgung zugrunde. In diesem Verständnis ist Überwachung eher negativ konnotiert und wird durchaus häufig in einen Zusammenhang mit Massenüberwachung, Überwachungsstaat oder Polizeistaat gestellt.

Einen anderen und vor allem sehr viel umfassenderen Überwachungsbegriff gibt es in den *Surveillance Studies:*[11] Überwachung bzw. Surveillance ist im Grunde jede Form von Informationsverarbeitung, in der soziale Akteure – Individuen, Gruppen, Organisationen – sich selbst oder ihre Umwelt beobachten und darauf basierend Entscheidungen treffen und handeln.[12] *New surveillance* ist Surveillance unter Verwendung neuer Datenerhebungs- und -verarbeitungstechniken sowie mehr und neuen Arten von Daten, die verarbeitet und genutzt werden.[13] Dieser breite Überwachungsbegriff, der in den Surveillance Studies rein beschreibend und gerade nicht wertend gemeint ist,[14] wird inzwischen weit über die Surveillance Studies hinaus genutzt – etwa für „Surveillance Capitalism"[15] –, hat dabei aber zugleich die stark negative Konnotation vom traditionellen liberalen, rein auf den Staat bezogenen Überwachungsbegriff geerbt. Und genau diesen Begriff nutzen nun die beiden anderen Arbeiten, die vom AKVorrat und die von Bieker et al., um ihren Untersuchungsgegenstand jeweils einzuführen. Dabei fallen zwei Dinge auf, die alles andere als unproblematisch sind: Erstens wird in beiden Fällen aus terminologischer Koinzidenz auf inhaltliche Identität der Begriffe geschlossen. Zweitens spiegelt sich in der jeweils nachfolgenden Darstellung der konkret zur Analyse herangezogenen Überwachungsmaßnahmen die Breite des eingeführten Überwachungsbegriffs nicht wider.

* *Der Autor bedankt sich bei Michael Plöse für die erkenntnisreiche Diskussion und die erhellenden Kommentare zu diesem Beitrag.*

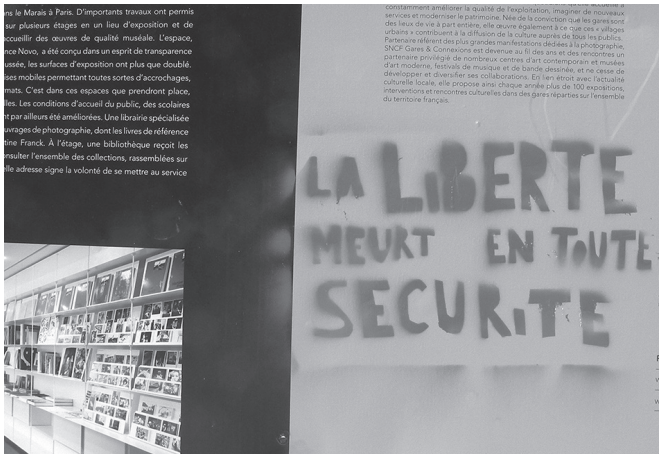
Alle vorliegenden Ansätze beschränken sich auf staatliche Überwachungsmaßnahmen, ob präventiv oder repressiv, ob von Polizeien und Geheimdiensten, vor dem Hintergrund der staatlichen Schutzpflichten für die eigenen BürgerInnen auch gegenüber Behörden anderer Staaten,[16] von der die Debatte um die ÜGR auslösenden Vorratsdatenspeicherung über die Videoüberwachung bis zum Entwurf für eine E-Evidence-Verordnung. Ausgeklammert werden dabei Maßnahmen im Sozial- und Gesundheitsbereich, im Arbeits- und Bildungsbereich oder in der AusländerInnenverwaltung, bei denen es sich um Überwachung im Sinne der Surveillance Studies handelt,[17] soweit nicht Strafverfolgungsbehörden und Geheimdienste auf dort vorhandene Daten zugreifen können. Die private, vor allem die privatwirtschaftliche Überwachung[18] wird nur soweit problematisiert, wie sie Anknüpfungsmöglichkeiten für staatliche Stellen bietet, ob durch Zugriff auf bei Privaten liegende Daten oder auf von diesen betriebene Kommunikationsinfrastrukturen.

… gesamt …

Alle betrachteten Vorschläge problematisieren den Umfang der zu erstellenden Analyse. Eine „Gesamtbetrachtung aller verfügbaren staatlichen Überwachungsmaßnahmen", wie es das BVerfG in der Entscheidung über die Vorratsdatenspeicherung forderte, wird teilweise als faktisch unmöglich,[19] teilweise auch als nicht wünschenswert angesehen.[20] Abgesehen von Versuchen einer möglichst umfassenden Darstellung der jeweils existierenden Überwachungsgesetze, -maßnahmen und -systeme Ende der 1970er[21] und Ende der 1980er Jahre[22] scheint es aktuell nur zwei vergleichbar umfassende Sammlungen zu geben – einerseits die Liste der österreichischen Überwachungsgesetze beim AKVorrat, andererseits die Sammlung zur Situation in der Bundesrepublik von Digitalcourage.[23] Moser-Knierim liefert zumindest eine Art Kriterienkatalog für die Auswahl der „Elemente, die den Grad gesamtgesellschaftlicher Überwachung prägen",[24] der allerdings so weit ist, dass es nichts geben kann, was nicht darunter fällt. Hingegen scheinen Roßnagel et al., Starnecker sowie die Bieker et al. davon auszugehen, dass wer immer zur Durchführung einer ÜGR verpflichtet sei, die Liste der Überwachungsgesetze und -maßnahmen selbst zusammenstellen müsse.

Das grundlegende Problem mit der Forderung nach einer tatsächlich gesamthaften Analyse der Überwachung liegt darin, dass sie entweder erstens Unmögliches verlangt, es zweitens keine Obergrenze geben kann, sie drittens zu einer arbiträren Entscheidung über die Inklusion oder Exklusion von gesetzlichen oder tatsächlichen Maßnahmen oder eingesetzten Techniken führt und darum keine sinnvolle Entscheidung erlaubt oder viertens sogar in einem *Whitewashing* endet.

Sie verlangt Unmögliches, wenn es sich um eine Gesamtanalyse der gesellschaftlichen Informationsverarbeitung handeln soll – das ist weit jenseits dessen, was selbst die Wissenschaft derzeit zu leisten in der Lage ist, wie sich unter anderem an den immer noch sehr oberflächlichen Versuchen zeigt, theoretischen Zugriff auf die *digitale Gesellschaft* zu gewinnen. Sie scheitert daran, dass eine echte Obergrenze fehlt: Wenn immer weitere Bereiche der Gesellschaft verdatet werden und zwar in immer höherer – sachlicher, zeitlicher und sozialer – Auflösung, dann verschiebt sich der Maßstab für Vollständigkeit immer weiter nach oben und relativiert dadurch den Umfang der existierenden Überwachung. Sie führt zu einer arbiträren Entscheidung über die Untersuchungsgegenstände, wenn sie zwar Gesamthaftigkeit der Überwachungsanalyse garantiert, sich aber dabei nur hinter der willkürlichen Auswahl des zugrunde gelegten Überwachungsbegriffes versteckt – und sich daran aufgrund der fundamentalen Umstrittenheit[25] von *Überwachung* aber nicht vorbeischmuggeln kann. Und sie wird – das zeigt ein Blick in die Geschichte – in Whitewashing enden: Ruprecht Kamlah hat schon vor vielen Jahren zweimal darauf hingewiesen, dass das BVerfG zwar immer von einem „unantastbaren Kernbereich privater Lebensgestaltung" spricht oder gar einer Intimsphäre als „unverletzlichem Innenraum, der von jedem staatlichen Eingriff freizuhalten ist, in den sich der Bürger vollkommen zurückziehen kann", aber beide seien in der Praxis leer.[26] Bieker et al. stellen richtig fest,[27] dass die Forderung nach einer wirklich umfassenden Analyse nicht zeigen kann, was sie nicht zeigen darf: dass nämlich der Rechtsstaat die Grenze der Rechtsstaatlichkeit überschritten hat.[28]



Freiheit stirbt mit Sicherheit, Foto: privat

… rechnung

Wirklich gerechnet werden soll nach keinem der Vorschläge, und wenn viel über Bewertung gesprochen wird, dann ist das gerade nicht quantitativ gemeint, sondern verweist immer nur darauf, dass der die ÜGR durchführende Akteur etwa eine „wertungsmäßige Betrachtung" vornehmen soll, „um das Bewusstsein für den Umfang der gesellschaftlichen Überwachung zu schärfen."[29]

Moser-Knierim, die auf Roßnagel et al. aufbaut und es erweitert, will in einer ÜGR untersuchen lassen, welche personenbezogenen Daten erstens der Staat „erhebt, erfasst und verarbeitet", zweitens bei Privaten vorhanden sind, auf die der Staat zugreifen kann, und wie drittens sich sowohl die Informations- und Kommunikationstechnik als auch das Nutzungsverhalten darstellt und entwickelt.[30]

Der Vorschlag für das Analyseverfahren vom AKVorrat ist einerseits sehr umfassend und detailliert – fast überdetailliert –, andererseits aber nur in Stichworten ausgearbeitet und an vielen Stellen lückenhaft. Darüber hinaus zielt das Verfahren vorläufig nur darauf ab, einzelne Gesetzesvorhaben zu bewerten

– die Entwicklung eines Verfahrens für eine „vollständige Evaluation im Sinne der ‚Überwachungs-Gesamtrechnung'" wird in die Zukunft verschoben.[31] Den am weitesten ausgearbeiteten Vorschlag liefert Starnecker mit seiner „modifizierten und konkretisierten" ÜGR, die er unter „Zugrundelegung der Erkenntnisse" aus der umweltökonomischen und der volkswirtschaftlichen Gesamtrechnung entwickelt habe,[32] deren starken Fokus auf Quantifizierung er aber nicht übernimmt. Starnecker untergliedert die ÜGR in drei Kategorien:[33]

1. Belastung – die deskriptive Beschreibung der Überwachungsmaßnahmen, systematisiert anhand der Kompetenzträger, Adressaten der Regelung sowie Anlasslosigkeit bzw. Anlassbezogenheit, mit Angaben zur Verwendungshäufigkeit;

2. Maßnahmen – grundrechtsschützende Maßnahmen und Instrumente, wobei er darunter insbesondere prozedurale und technische Schutzmaßnahmen *nach* dem (ersten oder primären) Grundrechtseingriff versteht, also etwa Trennung der Daten oder eine Zugriffskontrolle;

3. Zustand – die Untersuchung des „für den Bürger und die Gesellschaft verbleibende[n] Freiraum[s]" in Form einer „Bewertung und Abwägung aus den vorstehenden Kategorien".[34]

Einbezogen werden soll dabei in die Analyse des Zustands auch die Entwicklung der Technik und ihrer gesellschaftlichen Nutzung – wie viele andere Details ist das von Moser-Knierim übernommen.

Bieker et al.'s Vorschlag, an Stelle der ÜGR eine Gesetzes-Datenschutzfolgenabschätzung nach Art. 35 Abs. 10 DSGVO vorzunehmen, ist einerseits keine Alternative zur ÜGR, sondern stellt eine mögliche Operationalisierung dar, andererseits löst die Gesetzes-DSFA keines der drei von den Autoren am Ende ihres Beitrags genannten Probleme: die Unmöglichkeit, die gesamten Sicherheits- und Überwachungsmaßnahmen zu qualifizieren, die aussagekräftige und vergleichbare Bewertung der jeweiligen Einzelmaßnahmen sowie die Einführung einer „roten Linie".[35] Die Autoren widersprechen sich selbst: Einerseits müsse eine „reproduzierbare Methode zur Ermittlung der Gesamtüberwachung" erst entwickelt werden, damit „von Fall zu Fall vergleichbare Ergebnisse erzielt" würden,[36] andererseits verweisen sie gerade darauf, dass die Gesetzes-DSFA „eine fundierte Basis liefern [würde], um das Ausmaß der Überwachung zu beurteilen".[37]

In allen Vorschlägen bleibt der Bewertungsmaßstab unklar: Woraus ergibt sich bei einer Zusammenstellung aller Überwachungsmaßnahmen, wie groß die individuellen und gesellschaftlichen Freiräume noch bleiben? Zwar wollen sowohl Moser-Knierim als auch Starnecker den noch verbleibenden Freiraum explizit zu einem der Untersuchungsaspekte machen, aber wie? Starnecker verweist etwa darauf, dass „insbesondere auch soziologische Untersuchungen anzustellen" seien.[38] Das ist nur ein Verfahrens-, weder ein inhaltlicher noch ein Bewertungsvorschlag.

Beteiligte Akteure

Fast alle Vorschläge sehen den Gesetzgeber in der Pflicht, eine ÜGR durchzuführen, mit HEAT hingegen richtet sich der AK-Vorrat an die Österreichische Bundesregierung.[39] Roßnagel et al., Moser-Knierim und Starnecker schlagen vor, dass der Gesetzgeber die Bundesdatenschutzbeauftragte mit der eigentlichen Beobachtung und Bewertung der Gesamtüberwachungssituation beauftragen solle, möglicherweise unterstützt durch weitere Forschungs- oder TA-Institutionen. Das ist aus zwei Gründen höchst fragwürdig. Erstens sind Datenschutzaufsichtsbehörden massiv unterausgestattet[40] – eine Situation, die sich nur verschärfen würde, wenn ihnen auch die Aufgabe der Erstellung einer ÜGR übertragen würde. Zweitens ist darüber hinaus stark zu bezweifeln, dass sich an der bisher sowohl von Legislative wie Exekutive gezeigten Ignoranz gegenüber den Analysen, Stellungnahmen und Warnungen der Datenschutzaufsichtsbehörden überhaupt etwas ändern würde.

Ein weiterer Grund spricht dagegen, dem Gesetzgeber die Durchführung einer ÜGR zu überlassen: Abgesehen von einem *Hineinwachsen* in eine umfassende Überwachung durch „technische Veränderungen, veränderte Lebensbedingungen und Lebensweisen oder das Aufweichen der Eingriffsschwellen in der polizeilichen Praxis"[41] wird der Anknüpfungspunkt für die Durchführung einer ÜGR ein je konkretes Gesetzgebungsverfahren sein – gerade vor dem Hintergrund der großen Zahl der Gesetzgebungsverfahren im Überwachungsbereich. Der Gesetzgeber, der dieses Verfahren ja verfolgt, um eine Überwachung auszuweiten, hat darum natürlicherweise ein Interesse, die Gesamtüberwachung *klein zu rechnen* – das jeweils aktuell verhandelte Gesetz wird darum natürlich nie irgendeine *rote Linie* überschreiten. Das macht deutlich, dass die ÜGR eine strukturell dysfunktionale Anreizstruktur hat: Vollständigkeit zu garantieren, ist hart, der Gesetzgeber hat daran kein Interesse, und den Nachteil trägt die Gesellschaft.

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 co-leitet und sich unter anderem mit gesellschaftlichen Aushandlungen im Bereich Privacy, Surveillance, IT-Sicherheit und Datenschutz und deren Interpretation in verschiedenen Disziplinen und Theorieschulen befasst. Sein Forschungsinteresse gilt dem Schnittbereich von Informatik, Rechts- und Politikwissenschaft sowie Soziologie, dem Feld Informatik und Gesellschaft, der Modellifizierung und ihren gesellschaftlichen Auswirkungen sowie dem Datenschutz durch Technikgestaltung.

Zwei ÜGR-Verbesserungsvorschläge

Der erste Vorschlag betrifft eine Aufteilung der Verantwortung für die Durchführung der ÜGR, die mehr Anreize bietet. Dabei darf sie weder auf schwächere Akteure abgewälzt werden noch auf solche, die sich im Gesetzgebungsverfahren leicht ignorieren lassen. Der Gesetzgeber soll zur Durchführung der ÜGR verpflichtet werden, er darf sie aber nur auf der Basis von Listen von Überwachungsgesetzen und -maßnahmen vornehmen, die von unabhängigen Dritten erstellt werden, etwa Bundes- oder Landesdatenschutzbeauftragten, aber auch der Zivilgesellschaft.[42] Mit der Verantwortung würde auch Macht geteilt und so ließe sich verhindern, dass der Gesetzgeber einzelne Überwachungsmaßnahmen strategisch *übersieht* oder *klein rechnet*.

Der zweite Vorschlag zielt auf ein in der Verfassungsrechtsprechung inzwischen endemisches Problem: Das BVerfG beurteilt bei der Prüfung der Verhältnismäßigkeit von staatlichen (Überwachungs-)Maßnahmen schon seit langem weder Geeignetheit noch Erforderlichkeit.[43] In der Entwicklung des Datenschutzes wurde jedoch gerade dem Kriterium der Erforderlichkeit zentrale Bedeutung beigemessen,[44] bis hin zur Notwendigkeit eines formalen Nachweises:[45] „Eine Information ist zur Erfüllung einer Aufgabe erforderlich, wenn die Aufgabe ohne Kenntnis der Information nicht […] erfüllt werden kann.“[46] Oft sind diese Maßnahmen nicht einmal geeignet, die vom Gesetzgeber avisierten Ziele zu erreichen.[47] Wenn dem Staat nicht eine Beweispflicht für die Geeignetheit und Erforderlichkeit der beabsichtigten oder praktizierten Überwachungsmaßnahmen auferlegt wird, dann wird sich das BVerfG weiter in wolkigen Ergüssen zur Angemessenheit verlieren, die zu letztendlich arbiträren Ergebnissen führen[48] und die Grundrechte strukturell unterminieren.

Freiheitsbestandsanalyse

Das BVerfG hat im Urteil zur Vorratsdatenspeicherung statuiert, dass „die Freiheitswahrnehmung der Bürger nicht total erfasst und registriert werden“ dürfe und dies als zur verfassungsrechtlichen Identität der Bundesrepublik gehörig erklärt.[49] Der Ansatz der Freiheitsbestandsanalyse bildet das konzeptionelle Gegenstück zur ÜGR, indem er *Freiheit* als Startpunkt nimmt und *Überwachung* davon subtrahiert. Er analysiert die Nichterfassung und Nichtregistrierung der Freiheitswahrnehmung selbst – und nur sie.

Freiheit in Raesfeld, Foto: Frank Vincentz, CC BY-SA 3.0

Weil Freiheit ein ebenso fundamental umstrittener Begriff wie Überwachung ist, besteht der erste Schritt in der Operationalisierung von Freiheit. Wird die Verfassungsordnung strukturfunktionalistisch verstanden,[50] ist Freiheit die Menge der Gewährleistungsgehalte[51] der Grundrechte und grundrechtsgleichen Rechte, der deutschen wie der europäischen, sowie der zentralen freiheitsermöglichenden Verfassungsprinzipien wie Rechts- und Sozialstaatlichkeit und Demokratie.

Die Freiheitsbestandsanalyse zieht von den durch die grundrechtlichen Gewährleistungsgehalte sowie die Verfassungsprinzipien aufgespannten Freiheitsräumen jeweils die Überwachungsmaßnahmen ab. Sie ist Aufgabe des Gesetzgebers. Er sollte sie nicht, wie etwa Moser-Knierim vorschlägt,[52] an eine dritte „geeignete Stelle“ übertragen dürfen, da er damit seinen Rechtfertigungszwang in einem Institutionen- und Verfahrensdickicht in nichts auflösen könnte. Dann würde eine Auseinandersetzung um *Verfahrensfragen* die um den *Inhalt* verdrängen, etwa ob das Parlament die von Dritten angefertigte Analyse nur „zur Kenntnis nehmen“ oder „zustimmend zur Kenntnis nehmen“ muss. Der Gesetzgeber würde sich aus der Rechtfertigungspflicht für den in der Analyse abgebildeten Stand der verbleibenden gesellschaftlichen Freiheitsräume stehlen.[53] Ziel muss stattdessen sein, die konkreten rechtlichen Instrumente so auszugestalten, dass der Gesetzgeber gezwungen ist, sich einer *immanent politischen* Auseinandersetzung zu stellen.

Im Ergebnis muss der Gesetzgeber aufzeigen und begründen, welche Grundrechte und welche Freiheiten überhaupt noch und unter welchen Bedingungen überwachungsfrei, d. h. sowohl frei von tatsächlicher als auch von zu erwartender Überwachung, wahrgenommen werden können.

Die Kriterien für die Bewertung der Überwachungsgesetze, -maßnahmen und -praktiken enthalten viele von denen, die in der Diskussion um die ÜGR vorgeschlagen werden – etwa die Frage nach dem Überwachungsorgan, den Adressaten oder die nach Anlasslosigkeit/-bezogenheit, aber auch die Häufigkeit des Einsatzes der Maßnahmen in der Praxis[54] –, gehen aber darüber hinaus. Es gehört dazu, dass die Geeignetheit und Erforderlichkeit der Maßnahmen nicht nur behauptet, sondern tatsächlich nachgewiesen wurden und die Angemessenheit auf dieser Basis geprüft wurde. Weitere empirische Daten aus der Überwachungspraxis und über deren Auswirkungen sind in die Analyse aufzunehmen, wie Daten über Abschreckungseffekte auf das je konkrete Grundrecht und dessen Ausübung und die Identifikation der Hauptbetroffenen(gruppen) der spezifischen Überwachungsmaßnahmen: Es hängt eben nicht nur davon ab, wer als Adressat der Maßnahmen im Gesetzgebungsprozess identifiziert wird, sondern auch, ob in der Praxis vor allem bestimmte Gruppen betroffen sind – Grundrechte dienen nicht ausschließlich und nicht einmal primär dem Schutz einer Mehrheit, sondern im Kern dem Minderheitenschutz.[55]

Sowohl im Hinblick auf einzelne Grundrechte wie auf die verbleibenden Freiheitsräume insgesamt verschiebt die Freiheitsbestandsanalyse die Rechtfertigungslast von den Betroffenen auf den Staat. Für die Betroffenen wird Kritik an der Überwachung vereinfacht, weil sich Behauptungen des Gesetzgebers über die Existenz eines Freiheitsraumes diskursiv vergleichsweise leichter widerlegen lassen. *Ein* Beispiel für eine Überwachungsmaß-

nahme, die diesen Freiheitsraum einschränkt oder gar auflöst, verhindert, dass der Gesetzgeber auf diesen Freiheitsraum verweisen und damit eine echte oder vermeintliche Nicht-Allumfassendheit der Überwachung begründen kann.

Für den Staat wird die Rechtfertigungslast größer: Mit immer mehr Überwachungsmaßnahmen werden die Beispiele von *Räumen* für unüberwachte Freiheitswahrnehmung und deren Beschreibungen tendenziell immer unwahrscheinlicher, wenn nicht gar schlicht abstrus. Damit steigt nicht nur der Rechtfertigungszwang. Die Grenze dessen, was in einer Gesellschaft an Überwachung akzeptabel sein kann, lässt sich sinnvoll operationalisieren: Die Grenze ist erreicht, wenn die vom Gesetzgeber beschriebenen verbleibenden Freiheitsräume für unüberwachtes Wahrnehmen von Grundrechten jenseits der Lebenswirklichkeit der Menschen liegen. Wie immer umstritten Freiheit ist, – gesellschaftliche Zustände, die beschrieben werden als „keine permanente Überwachung der Bewegung von Menschen, die sich in Funklöchern befinden" oder „keine vollständige Überwachung der Kommunikation, wenn selbstkompilierte Messenger genutzt werden" lassen sich nicht mehr als Freiheit verkaufen.

Mit der Freiheitsbestandsanalyse wird damit die Rechtfertigungsordnung im Überwachungsbereich vom Kopf auf die Füße gestellt.

Anmerkungen

1 *BVerfGE 125, 260 – Vorratsdatenspeicherung.*
2 *BVerfGE 125, 260, 324.*
3 *Roßnagel, A. (2010). Die "Überwachungs-Gesamtrechnung" – Das BVerfG und die Vorratsdatenspeicherung. In: NJW 18/2010, S. 1238–1242, 1240.*
4 *Roßnagel, A. (2010), 1242.*
5 *Neben dem genannten Roßnagel (2010) vor allem Roßnagel, A.; Moser-Knierim, A. & Schweda, S. (2013). Interessenausgleich im Rahmen der Vorratsdatenspeicherung. Baden-Baden: Nomos, Kapitel 4.4. Beobachtungspflicht und Überwachungsgesamtrechnung.*
6 *Tschohl, C. et al. (2016). HEAT – Handbuch zur Evaluation der Anti-Terror-Gesetze. Wien: Arbeitskreis Vorratsdaten Österreich.*
7 *Starnecker, T. (2017). Videoüberwachung zur Risikovorsorge. Body-Cam zur Eigensicherung und Dashcam zur Beweissicherung – Eine verfassungs- und datenschutzrechtliche Analyse. Berlin: Duncker & Humblot.*
8 *Bieker, F.; Bremert, B. & Hagendorff, T. (2018). Die Überwachungs-Gesamtrechnung, oder: Es kann nicht sein, was nicht sein darf. In: Roßnagel, A.; Friedewald, M. & Hansen, M. (Hrsg.), Die Fortentwicklung des Datenschutzes – Zwischen Systemgestaltung und Selbstregulierung. Wiesbaden: Springer Vieweg. 139–150.*
9 *Hornung, G. & Schnabel, C. (2010). Verfassungsrechtlich nicht schlechthin verboten – Das Urteil des Bundesverfassungsgerichts in Sachen Vorratsdatenspeicherung. In: DVBl., 824–833, 827.*
10 *Starnecker, T. (2017). 365f.*
11 *Lyon, D. (2002). Editorial. Surveillance Studies: Understanding visibility, mobility and the phenetic fix. In: Surveillance & Society 1(1), 1–7. Eine recht umfassende Übersicht liefert Marx, G. T. (2015). Surveillance Studies. In: Wright, J. D. (Hrsg.). International Encyclopedia of the Social & Behavioral Sciences.,Amsterdam: Elsevier, 733–741.*
12 *Lyon, D. (1993). The Electronic Eye: The Rise of Surveillance Society. Minneapolis: University of Minnesota Press, 3ff.*
13 *Marx, G. T. (2002). What's New About the „New Surveillance"? Classifying for Change and Continuity. In: Surveillance & Society 1(1), 9–29.*
14 *Sewell, G. & Barker, J. R. (2001). Neither good, nor bad, but dangerous: Surveillance as an ethical paradox. In: Ethics and Information Technology 3, 181–194.*
15 *Zuboff, S. (2015). Big other: surveillance capitalism and the prospects of an information civilization. In: Journal of Information Technology 30, 75–89.*
16 *Vgl. Bieker et al. (2018), 145.*
17 *Vgl. Ball, K.; Haggerty, K. & Lyon, D. (Hrsg.) (2012). Routledge Handbook of Surveillance Studies. Abingdon: Routledge.*
18 *Vgl. Christl, W. (2017). Corporate Surveillance in Everyday Life – How Companies Collect, Combine, Analyze, Trade, and Use Personal Data on Billions. Wien: Cracked Labs – Institute for Critical Digital Culture.*
19 *Bieker et al. (2018), 144ff. im Hinblick auf sowohl die Auswahl als auch die Bewertung der zugrunde zu legenden Überwachungsmaßnahmen.*
20 *Sie könne zu einer „Überforderung des Gesetzgebers", gar zum „Stillstand im Bereich des Sicherheitsrechts" führen, so Starnecker (2017), 371.*
21 *Steinmüller, W. (1979). Der aufhaltsame Aufstieg des Geheimbereichs. In: Kursbuch 56, 169–198; Bölsche, J. (1979). Der Weg in den Überwachungsstaat. Reinbek: Rowohlt.*
22 *Kauß, U. (1989). Der suspendierte Datenschutz bei Polizei und Geheimdiensten. Frankfurt am Main: Campus Verlag.*
23 *https://digitalcourage.de/ueberwachungsgesamtrechnung/sammlung.*
24 *Moser-Knierim (2014), 365ff.*
25 *Gallie, W. B. (1956). Essentially Contested Concepts. In: Proceedings of the Aristotelian Society 56, 167–198.*
26 *Zuerst in Kamlah, R. (1970). Datenüberwachung und Bundesverfassungsgericht. In: Die Öffentliche Verwaltung 23(11), 361–364.*
27 *Bieker et al. (2018), 150.*
28 *Es ist darum wenig verwunderlich, dass Roßnagel et al. (2013), 178, diese Grenze erst „nahezu erreicht" sieht. Und selbst Bieker et al. (2018), 150, verweisen am Ende einfach auf das Verhältnismäßigkeitsprinzip und fordern, dass „umso strenger geprüft wird, desto schwerer der Eingriff wiegt."*
29 *Vgl. Moser-Knierim (2014), 237.*
30 *Moser-Knierim (2014), 237ff.*
31 *Tschohl et al. (2016), 11.*
32 *Vgl. Starnecker (2017), 371f.*
33 *Starnecker (2017), 373f.*
34 *Starnecker (2017), 374.*
35 *Bieker et al. (2018), 150.*
36 *Bieker et al. (2018), 145.*
37 *Bieker et al. (2018), 149f.*
38 *Starnecker (2017), 375.*
39 *Tschohl et al. (2016), 26.*
40 *„Defizitbericht" des Hamburgischen Datenschutzbeauftragten (2016), 25. Tätigkeitsbericht Datenschutz 2014/2015. Anhang „Zahlen – Fakten – Defizite – Lösungen".*
41 *Moser-Knierim (2014), 245.*
42 *Wie die Liste von Digitalcourage.*
43 *Hornung & Schnabel (2010), 826.*
44 *Podlech, A. (1973). Datenschutz im Bereich der öffentlichen Verwaltung. Beiheft 1, Datenverarbeitung im Recht (DVR). Berlin: J. Schweitzer Verlag, 54ff.*
45 *Podlech, A. (1982). Individualdatenschutz -- Systemdatenschutz. In: Brückner, K. & Dalichau, G. (Hrsg.), Beiträge zum Sozialrecht – Festgabe für Grüner., Percha: Verlag R. S. Schulz, 451–462, 455f.*
46 *Podlech, A. (1995). Der Informationshaushalt der Krankenkassen: Datenschutzrechtliche Aspekte. Baden-Baden: Nomos, 21.*
47 *Vgl. für den Einsatz von CCTVs zur Senkung der Kriminalität Welsh,*

B. C. & Farrington, D. P. (2002). Crime prevention effects of closed circuit television: a systematic review. UK Home Office Research, Development and Statistics Directorate.

48 Vgl. Kritik bei Schlink, B. (1974). Abwägung im Verfassungsrecht. Berlin: Duncker & Humblot.

49 BVerfGE 125, 260, 324.

50 Vgl. Luhmann, N. (1965). Grundrechte als Institution. Berlin: Duncker & Humblot.

51 Vgl. Rusteberg, B. (2009). Der grundrechtliche Gewährleistungsgehalt: Eine veränderte Perspektive auf die Grundrechtsdogmatik durch eine präzise Schutzbereichsbestimmung. Tübingen: Mohr Siebeck.

52 Moser-Knierim (2014), 244.

53 Zu dieser Pflicht vgl. BVerfGE 113, 273 – Europäischer Haftbefehl.

54 Vgl. Starnecker (2017), 373.

55 Steinmüller, W. (1971). Rechtspolitische Bemerkungen zum geplanten staatlichen Informationssystem. In: Würtenberger, T. (Hrsg.), Rechtsphilosophie und Rechtspraxis. Frankfurt am Main: Vittorio Klostermann, 81–87, 85.

Benjamin Derin

Überwachung, Polizei und ziviler Kontrollverlust

Von der falschen Sicherheit der Präventionsgesellschaft

Staatliche Überwachung und polizeiliche Befugnisse nehmen seit langer Zeit zu, ohne dass ihnen hinreichende Kontrollmöglichkeiten gegenübergestellt werden. Dabei gerät das den Rechtsstaat auszeichnende Verhältnis zwischen Eingriffs- und Abwehrrechten zunehmend aus dem Gleichgewicht. Das Streben nach vermeintlicher Sicherheit wird zur obersten Priorität. Damit einher geht ein sich veränderndes Fremd- und Selbstverständnis der Institution Polizei, die mit immer umfassenderen Aufgaben betraut wird, eine wachsende Rolle im öffentlichen Diskurs einnimmt und sich zugleich der zivilgesellschaftlichen Kritik und Kontrolle zu entziehen droht.

Von Staatstrojanern und Fußfesseln: Wildwuchs der Befugnisse

In den letzten Jahren ist eine massive Ausweitung der polizeilichen Befugnisse vor allem auf zwei sich teilweise überschneidenden Ebenen zu beobachten: zum einen bei der Nutzung technischer Überwachungsmethoden, zum anderen in der landesrechtlichen Gefahrenabwehr in Form der Polizeigesetze.

Neue technische Überwachungsmethoden

Nahezu am Fließband werden derzeit neue heimliche Ermittlungsmaßnahmen geschaffen und bestehende ausgeweitet: Mit der Online-Durchsuchung, Quellen-TKÜ und Telefonüberwachung, *stillen SMS, IMSI-Catchern* oder Funkzellenabfragen sowie der erleichterten Datenverwertung einschließlich algorithmengestützter Auswertung hat sich mittlerweile ein massives Arsenal an Überwachungswerkzeugen aufgehäuft. Diese Entwicklung kennzeichnet einerseits ein Zuwachs in der Breite – also neue Maßnahmen und Mittel – sowie andererseits eine zeitliche Vorverlagerung – also die Anwendung weit im Vorfeld konkreter Verdachtsmomente. Ein Ende der Aufrüstung ist nicht in Sicht. Mit der Begründung, der Staat müsse jede technologische Neuerung zur Verbrechensbekämpfung nutzen und drohe, gegenüber den Kriminellen und Terroristen ins Hintertreffen zu geraten (Stichwort *going dark*), hat sich bislang nahezu die gesamte Wunschliste durchsetzen lassen. Auch ohne ausdrückliche rechtliche Grundlage wird eingesetzt, was technisch möglich ist. Es scheint, dass sich Teile der Sicherheits- und Strafverfolgungsbehörden in einer Art Wildem Westen der digitalen Überwachung wähnen. Und angesichts der Verheißungen scheinbar unbegrenzter technischer Möglichkeiten besteht vielerorts offenbar nur ein geringes Bewusstsein für die Risiken, die mit derartigen Methoden einhergehen und für die Auswirkungen, die ihr Einsatz auf die Gesamtgesellschaft hat – von der Gefährdung der allgemeinen IT-Sicherheit durch den unreflektierten Umgang mit Sicherheitslücken und Staatstrojanern bis hin zur Schwächung der demokratischen Zivilgesellschaft durch ein Klima der Überwachung und Repression.

Bundesweite Reformen der Polizeigesetze

Auf dem Vormarsch sind diese modernen Eingriffsgrundlagen sowohl in der Strafprozessordnung (dort zur Strafverfolgung) als auch in den landesrechtlichen Polizeigesetzen (sie regeln komplementär die Abwehr allgemeiner Gefahren außerhalb des Strafrechts). Die seit 2017 anrollende und noch immer nicht abgeschlossene Welle neuer Polizeigesetze, die sich inzwischen auf nahezu alle Bundesländer ausgedehnt hat und zu denen etwa das umstrittene bayerische Polizeiaufgabengesetz gehörte, brachte daneben aber auch eine massive Ausweitung klassischer Befugnisse mit sich. Hierzu gehören je nach Bundesland etwa öffentliche Videoüberwachung, verdachtsunabhängige Kontrollen, Meldeauflagen, Hausarrest, Kontaktverbote, elektronische Fußfesseln, Taser[1] und monatelanger Präventivgewahrsam. Parallel dazu wurde – vor allem mittels des berüchtigten Konzepts der „drohenden Gefahr" – die Schwelle polizeilichen Eingreifens herabgesetzt, sodass die Polizei auf dem Gebiet der Gefahrenabwehr künftig früher Maßnahmen ergreifen darf und dabei weniger Anhaltspunkte dafür darlegen muss, dass die Person, gegen die sich diese Maßnahmen richten, tatsächlich eine Gefahr darstellte (s. Lippa 2018). Althergebrachte Kriterien, nach denen das Handeln der Polizei bislang juristisch beurteilt wurde, verschwimmen zusehends und schaffen immer größere Spielräume für die agierenden Beamten.

Dieser Bereich wirkt im Vergleich zu dem weiter oben beschriebenen High-Tech-Rüstzeug womöglich weniger bedeutsam und

zukunftsrelevant, hat aber durchaus weitreichende Implikationen. Schließlich sind es gerade diese etwas handfesteren Mittel, die von Polizisten tagtäglich tausendfach angewandt werden. Sie bilden damit auch die Basis für das Grundverständnis dessen, was die Polizei darf und was sie nicht darf – innerhalb der Polizei, im juristischen Diskurs und in der Öffentlichkeit. Wenn die polizeirechtlichen Eingriffsermächtigungen derart ausgeweitet werden, verändern sich sowohl die Rolle der Polizei in der Gesellschaft als auch ihr Verhältnis zu den Bürgern. Das zeitlich frühere Zugreifen mit vielfältigeren und heftigeren Methoden bei geringerem Rechtfertigungsdruck und ineffektiver externer Kontrolle lässt die Polizei als Institution mehr Raum im sozialen Gefüge einnehmen und macht sie in Begegnungen mit dem Einzelnen zunehmend unanfechtbar.

Das Primat der Prävention

Möglicherweise geht die Schaffung der neuen Befugnisse aber auch umgekehrt darauf zurück, dass der Polizei eine neue Rolle in der Sozialstruktur zugedacht wird. Die regelmäßig zur Begründung von Verschärfungen angeführte Behauptung, dass es der Polizei an den Waffen fehle, um ihre Aufgaben zu erfüllen, kann natürlich nur an diesen Aufgaben gemessen werden.

Hier zeigt sich, wie sehr sich das Verständnis des Polizeilichen gewandelt hat. Klassische Aufgabe der Polizei ist es, Straftaten zu verfolgen, nachdem sie begangen wurden, und Gefahren abzuwehren, wenn sie konkret bevorstehen. War das lange Zeit aus der Sicht von sowohl Bevölkerung als auch Politik und Behörden ausreichend, hat in den letzten Jahrzehnten ein Begriff an Bedeutung gewonnen, dem dies nicht genügen kann: Prävention. Der (wohl ohnehin zum Scheitern verurteilte) Versuch, durch die Bestrafung eines Täters weiteren Taten durch andere vorzubeugen, muss regelrecht rückständig anmuten gegenüber der Vorstellung, durch frühzeitige Einwirkung auf tatgeneigte Personen und ihre Umwelt schon den Keim der Tat ersticken zu können, bevor er sich entfaltet. Als übergreifende Idee zieht sich die Logik der Prävention durch die gesamte Gesellschaft – von Gesundheit und Drogen über Terrorismus und Naturkatastrophen bis hin zu Alltagskriminalität. Ganz allgemein formuliert, kann ein unerwünschtes Ereignis früher abgewehrt werden, wenn es früher erkannt wird. Das gelingt umso besser, je mehr über die Faktoren bekannt ist, die das Ereignis auslösen, und je effektiver die Mechanismen zu deren Identifizierung sind. Auf die Bereiche der Strafverfolgung und Gefahrenabwehr angewandt geht es demnach darum, Anhaltspunkte für potenzielle Taten möglichst frühzeitig festzustellen und für eine vorbeugende Intervention nutzbar zu machen.

Der gesellschaftliche und politische Anspruch an die heutige Polizeiarbeit ist es folglich immer, relevante Abläufe zu prognostizieren und zu verhindern. Spiegelbildlich zum Aufstieg des Präventionsgedanken ist der Bedeutungszuwachs des Topos *Sicherheit*. Die Formulierung bezieht sich heute nahezu ausschließlich auf die Abwehr terroristischer Gefahren und die Bekämpfung von Kriminalität, nicht auf vermutlich in vielerlei Hinsicht bedeutendere Themenfelder wie Sicherheit vor Arbeitslosigkeit, Klimawandel oder Einsamkeit. So verstandene Sicherheit wird angeblich hergestellt durch die Vorbeugung aller denkbaren Bedrohungen. Das ist besonders gefährlich, weil Sicherheit als hundertprozentige versprochen wird, was aber selbstverständlich nicht erreichbar ist, weshalb das Streben nach ihr keine natürlichen Grenzen hat. Die verstärkte Thematisierung des Präventions-und-Sicherheits-Komplexes löst entsprechend hohe Erwartungen in der Gesellschaft aus. Bevölkerung, Politik und Medien werden ungeduldiger im Umgang mit Risiken. Mit der nachträglichen Reaktion auf Straftaten gibt man sich konsequenterweise nicht mehr zufrieden, auch die Abwehr unmittelbar bevorstehender Gefahren genügt nicht. Das Primat der Prävention fordert vielmehr die Erkennung und Beseitigung der Gefahr zum frühestmöglichen Zeitpunkt – am besten, bevor sie überhaupt entstehen konnte. Für die Arbeit der Polizei muss das erhebliche Folgen haben: Sie ist auszurüsten mit Mitteln, die ihr ein weit vorgelagertes Identifizieren von Risiken im Wege der Prognose und ein möglichst frühes Eingreifen ermöglichen. Dabei spielt keine Rolle, ob die neuen Überwachungsmaßnahmen überhaupt geeignet sind, irgendetwas zu verhindern. Selbstverständlich wollen wir alle, dass Gewalttaten vermieden werden. Aber weder beim LKW-Anschlag am Breitscheidplatz noch den NSU-Morden oder dem Attentat in Halle scheiterte eine polizeiliche Intervention an mangelnden Befugnissen. In einem im Oktober 2019 nach fünf Jahren beendeten Mordprozess gegen zehn Angeklagte aus der Berliner Rocker-Szene hat die Polizei nach den Feststellungen des Gerichts mindestens fünf Tage vor der Tat u. a. durch gewöhnliche Telefonüberwachung von dem bevorstehenden Mord gewusst, aber nichts unternommen – möglicherweise, um die Ermittlungen nicht zu gefährden. Im Mordfall Walter Lübcke ist inzwischen bekannt geworden, wie viele Anhaltspunkte bei Geheimdiensten und Polizei auf die fortgesetzte Aktivität des Tatverdächtigen in der rechtsradikalen Szene bestanden, denen aber nicht nachgegangen wurde. Es scheint, dass es den Sicherheitsbehörden regelmäßig jedenfalls nicht an Eingriffsrechten fehlt.

Im politischen Diskurs ist das alles völlig unerheblich. Reflexartig wird im Namen der Sicherheit mehr Überwachung gefordert und gewährt. Während also die stetige Ausweitung der Befugnisse sicherlich die Rolle der Polizei verändert, hat andererseits der skizzierte grundsätzliche Wandel gesellschaftlicher Einstellungen seinerseits das Fundament für diese Entwicklung bereitet.

Ziviler Kontrollverlust

Die höchst problematische Zunahme von Eingriffsermächtigungen müsste eigentlich von einem entsprechenden Ausbau bürgerlicher Abwehr- und Kontrollmöglichkeiten begleitet werden. Ein solcher Ausbau findet aber nicht statt – im Gegenteil werden sogar just diese Rechte vielfach noch abgebaut. Das lässt sich in unterschiedlichen Bereichen beobachten.

Abbau von Beschuldigten- und Verteidigungsrechten

Wie erläutert erfolgt ein erheblicher Teil der hier behandelten staatlichen Informationsgewinnung zum Zwecke der Strafverfolgung. Dort stehen den Betroffenen, die dann regelmäßig Beschuldigte eines Strafverfahrens sind, spezifische Beschuldigtenrechte zu. Sie betreffen nicht nur den konkreten Rechtsschutz gegen belastende Maßnahmen wie Durchsuchungen, Verhaftung oder eben Überwachung, sondern unter anderem auch die

Beteiligung am Verfahren etwa durch das Recht, befangene Richter abzulehnen oder Beweisanträge zu stellen. Die bestehenden Abwehrrechte sind den derzeitigen Entwicklungen in der Praxis allerdings nicht gewachsen. Da es sich bei Überwachungsmaßnahmen grundsätzlich um heimliche Eingriffe handelt, bestehen dagegen nur selten effektive tatsächliche Abwehrmöglichkeiten. Dass ein Telefon abgehört oder der PC ausgeforscht wurde, erfahren Betroffene meist erst, wenn die Maßnahme beendet ist – und selbst dann nicht immer. Hier kann die klassische Rechtsschutzkonzeption nur bedingt Abhilfe schaffen, die Zielperson wird auf die nachträgliche Überprüfung teils Jahre nach den Ereignissen verwiesen. Hinzu tritt, dass moderne Technologien den Zugriff auf enorm viele und sehr sensible Informationen erlauben, die mithilfe immer leistungsfähigerer Auswertungs- und Speichermethoden auf ganz neue Weise nutzbar gemacht werden. Denn wo entgrenzte staatliche Überwachungsbefugnisse auf eine nahezu vollständig digitalisierte Gesellschaft treffen, werden plötzlich ganze Lebensläufe und Persönlichkeiten zu offenen Büchern. Das Auslesen eines Smartphones lässt heute oft ohne Weiteres auf Identität, Familie, Beruf, soziales Umfeld, Glaube, politische Einstellung, Hobbies, Interessen, sexuelle Orientierung usw. schließen und möglicherweise sogar auf mehr, als Nutzer selbst von sich wissen – so jedenfalls das Versprechen der sich dies zu Nutze machenden Daten- und Werbeindustrie. Wenn sich die Ermittlungsarbeit nun dramatisch in diesen Bereich hinein verschiebt – die Bedeutung von Erkenntnissen aus technischer Überwachung im Strafverfahren nimmt rasant zu – muss diesem technologischen Wandel angemessen Rechnung getragen werden. Die gegenwärtigen Reformen der Strafprozessordnung enthalten zwar regelmäßig Ausweitungen von Eingriffsbefugnissen, effektive neue Kontrollmechanismen finden sich dort allerdings nicht. Stattdessen werden die Handlungsspielräume der Beschuldigten und ihrer Verteidigerinnen und Verteidiger in der Hauptverhandlung immer weiter reduziert, indem beispielsweise die althergebrachten Rechte zur Ablehnung befangener Richter oder zum Anbringen eigener Beweisanträge fortlaufend beschränkt werden. So warnten die Strafverteidigervereinigungen jüngst, die im Mai 2019 durch das Kabinett angekündigte Strafprozessreform bringe Einschränkungen des Beweisantragsrechts, „wie dies zuvor nur in der rechtsstaatsfreien Zeit 1933-1945 der Fall war“ (Conen et al 2019). So wird der Staat mit immer neuen Befugnissen ausgestattet, während der Einzelne dem Staat gegenüber immer wehrloser wird.

Beschwerdestellen und Kennzeichnungspflichten

Das wachsende Ungleichgewicht zwischen staatlichen Ermächtigungen und bürgerlichen Abwehr- und Kontrollmöglichkeiten ist auch außerhalb von Strafverfahren, also im Polizeirecht festzustellen. Die oben genannte radikale Ausweitung der diesbezüglichen polizeilichen Handlungsspielräume unter dem alles überstrahlenden Dogma der Prävention führt dazu, dass der Polizei nicht nur eine Vielzahl neuer Mittel und Rechtsgrundlagen zur Verfügung steht. Deren Anwendung wird auch schwieriger überprüfbar, weil Voraussetzungen abgesenkt, Kriterien aufgeweicht und Eingriffszeitpunkte vorverlagert werden. Dass eine solche Entfesselung dramatische Folgen für Bürgerrechte und Demokratie haben kann, liegt auf der Hand. Umso wichtiger müsste es auch hier sein, einen derartigen Ausbau des Eingriffspotenzials – so er irrtümlich überhaupt für notwendig erachtet wird – wenigstens von zusätzlichen Kontrollmechanismen begleiten zu lassen. Die weitgehende Eindämmung staatlicher Willkür zählt immerhin zu den Fundamenten des Rechtsstaates und der freien Gesellschaft. Sie kann sich aber nicht in Deklarationen und Selbstbeweihräucherung erschöpfen („70 Jahre Grundgesetz!“), sondern muss effektiv gewährleistet werden. Und zwar genau gegenüber denen, die staatliche Macht ausüben.

Still not loving PAG, Foto: Günther Gerstenberg

Ganz entscheidende Bedeutung könnte hier zwei Mechanismen zukommen: unabhängigen Beschwerdestellen und der Kennzeichnungspflicht. Bei Beschwerdestellen handelt es sich um Instanzen, die eine Anlaufstelle für das Melden polizeilichen Fehlverhaltens bieten und damit dem Problem begegnen, dass in Deutschland dafür bislang vor allem die Polizei selbst zuständig ist. Wer beispielsweise einen unverhältnismäßigen Gewalteinsatz durch Polizisten rügen möchte, muss sich dafür an Polizisten wenden. Die Polizei ist allen empirischen Erkenntnissen nach nicht in der Lage, dieser doppelten Rolle als Ermittler und Beschuldigter zugleich gerecht zu werden. Verfahren wegen Körperverletzung im Amt werden ganz überwiegend und unverhältnismäßig oft eingestellt und führen so gut wie nie zu Verurteilungen. Viele Betroffene trauen sich nicht, einschlägige Vorfälle anzuzeigen; es wird mit einer erheblichen Dunkelziffer gerechnet (vgl. Abdul-Rahman et al 2019). Nicht zuletzt deshalb wird seit langem die Einrichtung unabhängiger Beschwerdestellen gefordert. In anderen Ländern ein erprobtes Mittel, schreitet die Umsetzung hier nur langsam voran. Häufig gehen die Konzepte auch nicht weit genug, um einen tatsächlichen Gegenpol zu gewährleisten: Von Bürgerrechtlern aufgestellte Kriterien enthalten insbesondere eine unabhängige Arbeitsweise außerhalb der Polizeiorganisation, ausreichende finanzielle Mittel und eigene Ermittlungsbefugnisse (vgl. die Eckpunkte bei Töpfer 2014). Ein weiteres wesentliches Instrument der zivilen Kontrolle stellt die Kennzeichnungspflicht dar. Auch sie ist in vielen Ländern weltweit anerkannt und wurde durch den EGMR nachdrücklich empfohlen, der in einem Urteil gegen die Bundesrepublik überdies feststellte, ohne eine verlässliche individuelle Kennzeichnung von Polizeibeamten könne in Prozessen wegen Polizeigewalt von einer effektiven Aufklärung nur schwerlich die Rede sein (Urteil v. 09.11.2017 – Hentschel und Stark ./. Deutschland). Dennoch wehren sich Interessenverbände der Polizei vehement gegen solche Kennzeichnungen, in denen sie nicht ganz ohne Ironie einen Ausdruck allgemeinen Misstrauens und eine unzulässige Generalverdächtigung sehen. Noch immer besteht nicht in allen Bundesländern eine Kennzeichnungspflicht.

Öffentlicher Diskurs

Diese Auseinandersetzungen verdeutlichen, dass sich auch der öffentliche Diskurs verschoben hat. Es ist inzwischen völlig alltäglich, dass sich die Polizei über ihre Funktionäre und Gewerkschaften als Institution an politischen Debatten von der Kriminal- bis hin zur Migrationspolitik beteiligt bzw. diese initiiert, sich in Gesetzgebungsverfahren positioniert, Pressearbeit macht und ganz allgemein meinungsbildend in die Gesellschaft hineinwirkt. Dass sie hierbei nicht neutral, sondern Partei ist, scheint nahezu vergessen. Für die Problematik wurde in letzter Zeit ein gewisses öffentliches Bewusstsein geweckt, weil zunehmend polizeiliche Fehlinformationen bekannt wurden. Der Deutsche Journalisten-Verband sah sich beispielsweise im Juli 2019 anlässlich falscher Angaben der Polizei über die Zahl verletzter Beamter nach der Besetzung eines Tagebaus in NRW dazu veranlasst, daran zu erinnern, dass es die Aufgabe von Journalisten ist, auch Polizeimeldungen kritisch zu hinterfragen. Und gegen die auf Twitter durch die Polizei veröffentlichte Falschbehauptung, bei der Räumung eines Kiezladens in Berlin habe für die Beamten aufgrund eines unter Strom gesetzten Türknaufs Lebensgefahr bestanden, ist dort Klage eingereicht worden. Dennoch wird die Polizei überwiegend als unparteiische und über jeden Zweifel erhabene Institution betrachtet und hat so gewaltigen Einfluss auf die öffentliche Meinung. Dieser Einfluss wird zur Erreichung bestimmter politischer Ziele eingesetzt – so etwa als Polizeigewerkschafter 2017 erreichten, dass der Deutsche Gewerkschaftsbund dem im Münchner DGB-Haus geplanten Antifa-Kongress vorübergehend die Räume kündigte und 2018 in Berlin der Vortrag einer Anwältin über den G20-Gipfel aus dem IG-Metall-Haus geworfen wurde. Die Polizei verfügt auch über eine starke Lobby, wenn es um die eigenen Belange geht. Dies ist an der Auseinandersetzung um Kennzeichnungspflicht, Beschwerdestellen und Polizeigewalt zu sehen. Weiteres Beispiel ist die auf Drängen der Polizeigewerkschaften geschlossene Dienstvereinbarung für die Bundespolizei aus dem Februar 2019, wonach Bodycam-Aufzeichnungen bei Vorwürfen gegen die Polizei nicht für interne Ermittlungen genutzt werden dürfen.

Insgesamt zeigt sich hier ein problematisches (Selbst-)Verständnis der Polizei als einer von Kontrolle und Überprüfung weitgehend zu bewahrender Behörde, der im gerechten Kampf nicht die Hände gebunden sein dürfen und der es nicht zum Vorwurf gemacht werden dürfe, wenn sie ein wenig über das Ziel hinausschießt. Das hat dazu geführt, dass sich dort keine produktive Fehlerkultur entwickeln konnte und auf jedwede Kritik mit Ablehnung und Gegenangriffen reagiert wird. Dabei gehört eine kritische Betrachtung staatlicher Machtausübung zu den elementaren Grundsätzen jeder die Grund- und Menschenrechte ernstnehmenden Gesellschaftsordnung. Wenn gewisse führende Polizeigewerkschafter angesichts aufkommender Vorwürfe rechter Umtriebe und Rassismus nur erwidern:

> *„Die größte Menschenrechtsorganisation in Deutschland ist nicht Amnesty International, sondern die deutsche Polizei“*[2],

dann zeugt das von einem brisanten Rechts- und Selbstverständnis.

Fazit

Staatliche Überwachung ist einerseits im Kontext polizeilicher Befugnisse und ziviler Abwehrmöglichkeiten, andererseits vor dem Hintergrund grundsätzlicher gesellschaftlicher Entwicklungen zu betrachten. Die besorgniserregende Ausweitung entsprechender Eingriffsermächtigungen ist kein Zufall, sondern logische Konsequenz einer gesamtgesellschaftlichen Umorientierung entlang der Begriffe Sicherheit und Prävention. Der im Zuge dieser Umorientierung betriebene Ausbau des Überwachungs- und Sicherheitsapparates wird nicht einlösen können, was er verspricht. Er droht vielmehr, ausgerechnet das zu beschädigen, was an seiner statt notwendig und angebracht wäre: die Stärkung ziviler, demokratischer und freiheitlicher Kultur und Strukturen.

Referenzen

Abdul-Rahman L., Espín Grau H., Singelnstein T. (2019) Polizeiliche Gewaltanwendungen aus Sicht der Betroffenen. Zwischenbericht zum Forschungsprojekt „Körperverletzung im Amt durch Polizeibeamt*innen“ (KviAPol)

Conen S., Pollähne H., von Schlieffen J., Uwer T. (2019) Stellungnahme der Strafverteidigervereinigungen: „Eckpunkte zur Modernisierung des Strafverfahrens“

Lippa M. (2018) Drohende Gefahr: Konkrete Gefahr für die Freiheitsrechte. Bürgerrechte & Polizei/CILIP 117:11-19

Töpfer E. (2014) Unabhängige Polizei-Beschwerdestellen. Eckpunkte für ihre Ausgestaltung

Anmerkungen

1 *Distanz-Elektroimpulsgerät oder Elektroschock-Waffe*

2 *taz am Wochenende v. 12.12.2015, „Die Stimmungskanone“, S. 8-9; dw.com v. 9.6.2019, „Amnesty kritisiert Rassismus bei Behörden“, https://www.dw.com/de/amnesty-kritisiert-rassismus-bei-beh%C3%B6rden/a-19317756-0 (zuletzt abgerufen am 22.10.2019)*

Benjamin Derin

Benjamin Derin ist Rechtsanwalt in Berlin und Redakteur der Zeitschrift *Bürgerrechte & Polizei/CILIP.*

NETZPOLITIK.ORG

Alexander Fanta – Interview mit Peter Wedde

Überwachung am Arbeitsplatz: „Das Kontrollpotential ist riesengroß“

Der Arbeitsrechtler Peter Wedde berät seit Jahren Betriebsräte und Beschäftigte in Datenschutzfragen. Er warnt vor einer Ausbreitung der Überwachung am Arbeitsplatz. Deutschland brauche endlich ein eigenes Gesetz für den Beschäftigtendatenschutz, sagt Wedde im Interview.

netzpolitik.org: *Wir haben zuletzt berichtet, dass Behörden immer mehr Fälle von fragwürdigem GPS-Tracking im Firmenwagen und Videoüberwachung am Arbeitsplatz[1] gemeldet werden. Man bekommt den Eindruck, dass die Möglichkeiten zur Kontrolle durch den Arbeitgeber ständig wachsen. Lässt sich das aus Ihrer Praxis bestätigen?*

Peter Wedde: Ja. Die technischen Kontrollmöglichkeiten haben in einem Maß zugenommen, das vor ein paar Jahren nicht vorstellbar war. Es gibt heute fast kein Berufsfeld mehr, in dem nicht automatisch IT-mäßige Kontrollen im Hintergrund ablaufen, selbst in typischen Handwerksbetrieben. In vielen Fällen erfolgen hier allerdings keine vorsätzlichen Auswertungen durch Arbeitgeber, aber die Möglichkeit hierzu besteht. Und wenn die Möglichkeit für Kontrollen besteht, dann erfolgen sie vielfach über kurz oder lang auch.

Heute gibt es viele technische Gelegenheiten zur Kontrolle, etwa beim Auto, um zu schauen, wie schnell die Mitarbeiter gefahren sind und wo sie waren. Es ist nicht überraschend, dass Chefs dann sagen: Jetzt will ich mal gucken, ob die vom Mitarbeiter ausgefüllte Arbeitszeit mit der Realität übereinstimmt. Das Kontrollpotential ist riesengroß.

netzpolitik.org: *Unsere Umfrage hat gezeigt, dass viele Firmen auf fragwürdige Kontrollmöglichkeiten setzen. Welche Formen der Überwachung sehen Sie in Ihrem Alltag am häufigsten?*

Peter Wedde: Videoüberwachung ist in erschreckend vielen Firmen ein Thema. Kameras werden häufig in unzulässiger Weise zur Kontrolle eingesetzt. Das fängt an beim Bäckerladen, wo über der Kasse verdeckt eine kleine Kamera angebracht ist, um zu sehen, ob die Verkäufer mit den Kassenbeständen sauber umgehen.

Häufig ist auch das GPS-Tracking, dass Sie angesprochen haben. In vielen Autos finden sich GPS-Transponder, deren Daten ausgewertet werden können. Diese Möglichkeit nutzen Arbeitgeber.

Ein anderer „Klassiker“ ist, dass in Firmen ohne Wissen der Beschäftigten Listen dazu erstellt werden, wer etwa die besten Verkäufer sind. Solche „Rennlisten“ sollte es eigentlich gar nicht geben.

Neuerdings gibt es immer öfter auch Auswertungen in neuen Kommunikationsanwendungen. Nehmen Sie beispielsweise ein internes Soziales Netzwerk, wie es viele Firmen inzwischen nutzen. Da kann ich beispielsweise wunderschön auswerten, wer wie viel kommuniziert und wer wie viele Likes für seine internen Geschichten bekommt. Wer sind die angesehensten Leute, wen kann keiner leiden? Das sind alles Dinge, die in Auswertungen einfließen und die jetzt in letzter Zeit im Kommen sind, muss man sagen. Das ist auch eine Verhaltenskontrolle.

Der Arbeitsrechtler Peter Wedde bei der Verleihung des Big-Brother-Awards in Bielefeld, Foto: Elelelevеn, CC BY-SA 2.0

netzpolitik.org: *Wie ist derzeit die Rechtslage bei diesen Beispielen? Darf ein Arbeitgeber einfach so seine Mitarbeiter filmen und im Auto tracken, wenn er das für notwendig hält?*

Peter Wedde: Ich halte heimliche Kontrollmaßnahmen aus verfassungs- und arbeitsrechtlichen Gründen grundsätzlich für unzulässig. Und selbst offene Kontrollmaßnahmen, etwa mit sichtbar angebrachten Kameras, sind nach der Rechtsprechung des Bundesarbeitsgerichts unzulässig, wenn sie dauerhaft ohne zwingenden Grund erfolgen. Permanent gefilmt werden darf nur, wenn es dafür ein sachliches Erfordernis gibt, zum Beispiel am Geldschalter einer Bank oder in Betriebsbereichen, in denen gefährliche Prozesse ablaufen. Dort sind dauerhafte Videokontrollen zum Schutz der Sicherheit von Beschäftigten erlaubt.

netzpolitik.org: Derzeit lesen wir häufig von Bedenken wegen Microsoft Office 365[2]. Das schlägt ja gerade in vielen Betrieben auf. Was für Probleme sehen Sie mit Office 365?

Peter Wedde: Office 365 ist eine Sammlung von Anwendungen, die die Firma Microsoft anbietet. Dazu gehören Standardbüroarbeitsmittel wie Word und Powerpoint, Archivsysteme wie

Sharepoint oder Kommunikationsanwendungen wie Skype oder Teams. Microsoft ist mit seiner Office-365-Oberfläche der geniale technische Coup gelungen, die unterschiedlichsten Anwendungen automatisch und komfortabel miteinander zu verbinden. Anwendern wird eine ständig aktualisierte und ergänzte bunte Welt von Büroanwendungen zur Verfügung gestellt, von denen Microsoft sagt, dass sie perfekt zusammenarbeiten.

Das Problem ist, dass bei der Arbeit mit allen diesen Anwendungen ständig personenbezogene Daten anfallen, die mit ebenfalls von Microsoft angebotenen Tools auswertet werden können. Damit wird zunächst einmal der persönliche Komfort erhöht. Wer mit Office 365 arbeitet, der bekommt bei einer entsprechenden Einstellung des Systems beispielsweise Vorschläge zu anderen Dateien angezeigt, die sie oder er vielleicht ebenfalls gebrauchen könnte. Das wird von vielen Menschen nicht als Kontrolle empfunden, sondern als Komfortgewinn.

Gleichzeitig sind aber auch Auswertungen dazu möglich, wer bestimmte Aufgaben wann erledigt hat oder welche Arbeiten noch offen sind. Selbst die Reihenfolge der Arbeitserledigung kann für Dritte nachvollziehbar sein.

Man kommt an der Feststellung nicht vorbei, dass Microsoft mit Office 365 eine gigantische Anwendung gebaut hat, die technisch faszinierend ist, die aber zugleich Kontrollmöglichkeiten bietet, von denen wir früher nicht zu träumen wagten.

netzpolitik.org: *Bei unrechtmäßiger Überwachung von Beschäftigten sind die Datenschutzbehörden der Länder zuständig. Doch unsere Rundfrage hat ergeben, dass die Behörden kaum Strafen wegen solcher Verstöße austeilen – die Firmen kommen meist mit einer Verwarnung davon. Glauben Sie, dass die Behörden ihren Auftrag erfüllen?*

Peter Wedde: Das, was die Aufsichtsbehörden in Deutschland an Arbeit machen, schätze ich sehr. Sie machen mit der knappen personellen und sachlichen Ausstattung, die sie haben, einen guten Job. Aber ich halte die Behörden für chronisch unterbesetzt. Das waren sie schon, bevor die Datenschutzgrundverordnung (DSGVO) vor eineinhalb Jahren wirksam wurde. Landesdatenschutzbeauftragte haben immer wieder und berechtigt gesagt: Wir brauchen mehr Mitarbeiter und mehr sachliche Mittel.

Was den Datenschutz von Beschäftigten angeht, ist das für die Aufsichtsbehörden allerdings nur eines von vielen wichtigen Themen. Aufgrund der notwendigen Spezialisierung kennt sich deshalb leider nicht jeder dort beschäftigte Datenschutzexperte auch im Arbeitsrecht gut aus. Das führt dazu, dass die notwendige Vernetzung der unterschiedlichen Rechtsgebiete und der dort bestehenden Probleme teilweise nur unzureichend gelingt. Das geht auf Kosten eines wirksamen Beschäftigtendatenschutzes.

Dazu kommt auch, dass den staatlichen Aufsichtsbehörden oft eine starke und nachhaltige politische Rückendeckung fehlt. Einen Verstoß bei einem großen Unternehmen zu monieren, der vielleicht zu wirtschaftlichen Konsequenzen wie Steuerausfällen oder Arbeitsplatzverlusten führt – das vermeidet der eine oder die andere Landesdatenschutzbeauftragte dann lieber doch. Zumal man dann davon ausgehen muss, dass eine Aufsichtsbehörde sich nach der öffentlichkeitswirksamen Verhängung einer hohen Geldbuße sehr schnell mit einer Phalanx von Anwälten aus international aufgestellten Anwaltsfirmen konfrontiert sieht, die alle möglichen Rechtsmittel einlegen.

Meine Erfahrung aus der Praxis ist zudem, dass die Datenschutzaufsichtsbehörden sich bei Fragen an der Schnittstelle zwischen Datenschutz- und Arbeitsrecht vielfach sehr zurückhalten. Wenn sich Beschäftigte oder Betriebsräte an die zuständige Aufsichtsbehörde wenden und einen Datenschutzverstoß melden, erleben sie immer wieder, dass versucht wird, das Thema erst einmal „runterzukochen“, um es vorsichtig zu sagen.

netzpolitik.org: *Was bedeutet das für die Betroffenen?*

Peter Wedde: Vertreter der Aufsichtsbehörden raten dann, das Thema erst einmal betrieblich zu klären. Wenn daraufhin der Hinweis kommt, dass das längst passiert sei und dass der Arbeitgeber nichts ändere, ist die Begeisterung von Aufsichtsbehörden, in derartige arbeitsrechtliche Konflikte reinzugehen, nicht sonderlich groß ist.

Dass da nicht mehr passiert und dass der Beschäftigtendatenschutz bei den Aufsichtsbehörden keine überragende Priorität hat, halte ich mit Blick auf die zu schützenden Rechte von mehr als 33 Millionen abhängig Beschäftigten für ein ganz grundsätzliches Problem.

Eine mögliche Lösung wäre eine unabhängige Aufsichtsbehörde für Beschäftigtendatenschutz, die sich nur um Datenschutz für abhängig tätige Arbeitnehmer kümmern. Eine solche Idee trifft aber im politischen Raum nur auf wenig Begeisterung, weil sie zunächst einmal Geld kosten würde. Die Wirtschaft lehnt sie völlig ab, wohl weil ein gesetzeskonformer Beschäftigtendatenschutz in vielen Betrieben immer noch fehlt.

Alexander Fanta und Peter Wedde

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[3]) und unter *@FantaAlexx* erreichbar.

Peter Wedde ist Professor für Arbeitsrecht und Recht der Informationsgesellschaft an der *Frankfurt University of Applied Sciences*, wissenschaftlicher Leiter der Beratungsgesellschaft *d+a consulting GbR* in Eppstein[4] und wissenschaftlicher Berater des Anwaltsbüros *Steiner Mittländer Fischer* in Frankfurt. Er berät Betriebsräte und Arbeitnehmer zum Thema Beschäftigtendatenschutz.

netzpolitik.org: *Im Koalitionsvertrag von Union und SPD steht, dass die Regierung ein eigenes Gesetz für den Beschäftigtendatenschutz zumindest prüfen möchte. Was sollte so ein Gesetz mindestens leisten?*

Peter Wedde: Das „wir prüfen" im Koalitionsvertrag verpflichtet die aktuelle Regierung nicht zum Handeln. In früheren Koalitionsverträgen gab es deutlichere Vorgaben für ein solches Gesetz, ohne dass etwas passierte. Die letzte CDU-/FDP-Regierung hatte sogar einen wenig beschäftigtenfreundlichen Entwurf auf den Weg gebracht, diesen dann aber kurz vor der Bundestagswahl zurückgenommen.

Was müsste in einem Beschäftigtendatenschutzgesetz stehen, das diesen Namen verdient? Beispielsweise verbindliche Vorgaben dazu, welche Daten bei Bewerbern erhoben werden dürfen wie etwa Informationen zur Berufsausbildung und welche Themen nicht abgefragt werden dürfen, etwa Aussagen zur Partei- oder Gewerkschaftszugehörigkeit oder zur sexuellen Orientierung.

Bezogen auf bestehende Beschäftigungsverhältnisse müsste festgelegt werden, ob und wie weit ein Arbeitgeber Beschäftigte durch heimliche oder offene Maßnahmen kontrollieren darf.

Sind Kontrollen zulässig, müsste beispielsweise geregelt werden, wie intensiv sie sein dürfen. Was gilt für den Umgang mit Gesundheitsdaten? Wie dürfen vorhandene Beschäftigtendaten verwertet oder mit anderen verknüpft werden?

Offen ist auch: Wie können sich von ihrem Arbeitgeber abhängige Arbeitnehmer gegen unzulässige Datenverarbeitung wehren? Wie müssen sie informiert werden? Wer hilft ihnen bei Unklarheiten? Das müsste alles in einem Beschäftigtendatenschutzgesetz geregelt werden.

Und dann ein ganz wichtiger Punkt: Wie ist es eigentlich mit spezifischen Mitbestimmungsrechten von Betriebs- und Personalräten zum Datenschutz? Sie können zwar bei der Einführung und Änderung von technischen Einrichtungen mitbestimmen, die zur Verwaltung von Verhaltens- und Leistungskontrollen bestimmt sind. Da haben die ein starkes Recht. Aber wenn es um Datenschutz selber geht, fehlt ein gesetzliches Mitbestimmungsrecht. Hierauf weisen Arbeitgeber im Streitfall regelmäßig hin.

netzpolitik.org: *Welche Fragen sollte ein neues Gesetz beantworten, um auch in Zeiten von maschinellem Lernen und sogenannter Künstlicher Intelligenz zukunftsfähig zu sein?*

Peter Wedde: Auch auf neue Fragen müsste ein Beschäftigtendatenschutzgesetz eine Antwort finden. Die DSGVO gibt beispielsweise vor, dass Datenverarbeitung für die betroffenen Personen transparent erfolgen muss. Wie das bei durch Algorithmen gesteuerten KI-Systemen funktionieren soll, deren genaue Funktionsweise oft ein Firmengeheimnis ist? Das weiß kein Mensch.

Wenn tatsächlich irgendwann das längst überfällige Beschäftigtendatenschutzgesetz verkündet würde, werden mir einzelne Regelungen darin wahrscheinlich nicht gefallen. Aber wir hätten dann immerhin mal Rechtsklarheit. Ich glaube, auch die Arbeitgeberseite wünscht sich, dass der Gesetzgeber zu bestimmten Themen klare Vorgaben schafft. Dann kann man sich je nach Position ärgern oder freuen, aber es würde viel, viel Energie frei, die im Moment durch Rechtsstreitigkeiten bezüglich des Umgangs mit personenbezogenen Beschäftigtendaten gebunden ist.

Quelle: https://netzpolitik.org/2019/ueberwachung-am-arbeitsplatz-das-kontrollpotential-ist-riesengross/

Anmerkungen

1 *https://netzpolitik.org/2019/wie-deutsche-firmen-ueberwachen/*
2 *https://mmm.verdi.de/medienwirtschaft/microsoft-und-der-datenschutz-61605*
3 *http://pool.sks-keyservers.net/pks/lookup?op=get&search=0x2271FE6D4CD84C62*
4 *http://s388989275.website-start.de/über-uns/prof-dr-peter-wedde/*

Chris Köver und Ingo Dachwitz

Datenethikkommission – RegierungsberaterInnen fordern strengere Regeln für Daten und Algorithmen

Eine Ethikkommission der Regierung sollte Antworten auf einige der kniffeligsten Fragen zum Umgang mit Daten und Algorithmen liefern. Trotz vieler Themen und kurzer Zeit fällt die Leistung der Kommission beachtlich aus. Ihr Bericht fordert neue Aufsichtsbehörden, eine Algorithmenverordnung auf EU-Ebene und eine „Pluralismuspflicht" für Social-Media-Torwächter.

Falls es nichts wird mit der Regulierung von Algorithmen: an der Arbeit der Datenethikkommission (DEK) liegt es schon mal nicht. Die 16 Mitglieder haben Beachtliches abgeliefert, vor allem, wenn man bedenkt, dass sie dafür nur ein Jahr Zeit hatten. Sie empfehlen der Regierung gleich eine ganze Palette von neuen Regelungen. Dazu gehört etwa eine Kennzeichnungspflicht, ein Zulassungsverfahren und Transparenzpflichten für Algorithmen mit einem hohem Risiko und eine neue Verordnung auf EU-Ebene, die all das bis ins Detail regeln soll. Das steht in dem Gutachten[1], das die Kommission heute[2] im Justizministerium vorstellt und das netzpolitik.org vorliegt

Der Druck auf die Kommission war gewaltig. Als die Bundesregierung sie vor einem Jahr mit dem Auftrag zurück ließ, die „ethischen Leitplanken" zu definieren „für den Schutz des Einzelnen, die Wahrung des gesellschaftlichen Zusammenlebens

und die Sicherung und Förderung des Wohlstands im Informationszeitalter", hatte man den Eindruck, das könnte ein kleines bisschen viel werden. Noch dazu für ein Gremium, dessen Mitglieder – darunter Fachleute für Ethik, Rechtswissenschaft, Informatik, Wirtschaft und Verbraucherschutz – ehrenamtlich arbeiteten. Hinter vorgehaltener Hand erzählten Mitglieder, ihre Familien hätten ihnen verboten, so etwas nochmal zu machen.

Das Ergebnis aber ist beachtlich geworden. Grob unterteilt ist das Papier in einen Teil zu Datenthemen und eine Teil zu algorithmischen Systemen, auch wenn sich beides nicht sauber trennen lässt. Im Blick hat die Kommission dabei vor allem auf die Praktiken von Unternehmen gerichtet und wie diese durch den Staat demokratisch eingehegt werden können. [Lest hier auch unseren Kommentar zum Gutachten der Datenethikkommission: 200 Seiten Erwartungsdruck[3] siehe Seite 49.]

Im Zweifel verbieten

Die Forderungen der ExpertInnen sind wesentlich ambitionierter als bisherige Leitlinien und werden an einigen Stellen bemerkenswert konkret. Ihre Regeln für algorithmische Systeme etwa wollen sie auf der Ebene der EU verankert haben, in einer neuen Verordnung, für die sie bereits einen Namen mitliefern: EUVAS. Je nach „Schädigungspotential" eines Systems sollen dort nach fünf Stufen verschiedene Regeln festgeschrieben werden.

Das reicht von einer verpflichtenden Abschätzung der Risikofolgen und Transparenzpflichten für Systeme mit „gewissem Schädigungspotential" bis hin zu Zulassungsverfahren oder gar Verboten für hochriskante Anwendungen. In solchen Fällen rät das Gremium zu „verschärften Kontroll- und Transparenzpflichten bis hin zu einer Veröffentlichung der in die Berechnung einfließenden Faktoren und deren Gewichtung, der Datengrundlage, sowie die Möglichkeit einer kontinuierlichen behördlichen Kontrolle über eine Live-Schnittstelle zum System".

Für die Aufsicht über diese Regeln empfiehlt sie, die bereits bestehenden Aufsichtsbehörden für diese Aufgabe fit zu machen und mit mehr Personal auszustatten. Zusätzlich soll eine neue Meta-Stelle – das „Bundesweite Kompetenzzentrum Algorithmische Systeme" – geschaffen werden, die die Aufsichtsbehörden bei ihrer Aufgabe unterstützen kann.

Als Beispiel nennt der Bericht etwa algorithmische Preissysteme im Onlinehandel, die Aufsichtsbehörden mit statistischen Tests prüfen könnten, um zum Beispiel Diskriminierung gegen Frauen zu verhindern. Auch sonst müssten Menschen vor Diskriminierung geschützt werden, stellt der Bericht klar, besonders dort, wo algorithmische Systeme zum Einsatz kommen, um menschliche Entscheidungen zu unterstützen oder zu ersetzen. An dieser Stelle empfehlen die ExpertInnen, das Allgemeine Gleichstellungsgesetz entsprechend zu überarbeiten und auf die Eigenheiten automatisierter Entscheidungen auszudehnen.

Gütesiegel[4], Verhaltenskodizes und andere Verfahren der Selbstregulierung von Unternehmen, wie sie derzeit im Trend liegen[5], finden die ExpertInnen ebenfalls sinnvoll. Schließlich müsse man nicht alles mit Gesetzen regeln. Sie könnten allerdings einen Gesetzesrahmen nicht ersetzen.

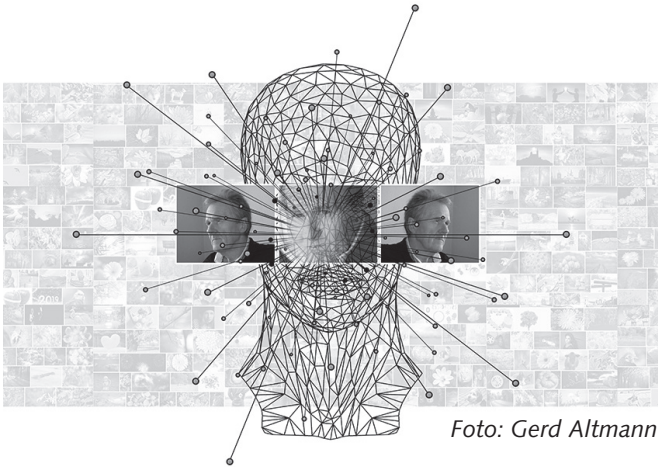


Foto: Gerd Altmann

„Alle Arten algorithmischer Systeme"

Im Fragenkatalog[6] der Bundesregierung war noch die Rede von „Künstlicher Intelligenz" einerseits und „algorithmenbasierten Prognose- und Entscheidungsprozessen" andererseits. Diese Unterscheidung reißt die Kommission gleich zu Beginn selbstbewusst ein: Es sei technisch nicht sinnvoll, über ethische Regeln nur für KI zu sprechen, da viele der Probleme ebenso für solche algorithmische Systeme gelten, die viel einfacher gestrickt sind. „Insofern beziehen sich die folgenden Ausführungen auf alle Arten algorithmischer Systeme", schreibt sie.

Auch warnt die Kommission davor, auf einzelne Algorithmen zu schauen. „Für die ethische Beurteilung kommt es jeweils auf das gesamte sozio-technische System an, also alle Komponenten einer algorithmischen Anwendung einschließlich aller menschlichen Akteure, von der Entwicklungsphase bis hin zur Implementierung in einer Anwendungsumgebung und zur Phase von Bewertung und Korrektur." Das ist sinnvoll, denn die Gefahr eines Algorithmus liegt in der Regel nicht in diesem selbst, sondern dem Kontext, in dem es eingesetzt wird, Darauf wies etwa die zivilgesellschaftliche Wächtergruppe AlgorithmWatch hin[7] – und wurde offenbar gehört.

Für Plattformen wie Facebook oder YouTube, im Bericht „Torwächter" genannt, empfiehlt der Bericht „ein ganzes Spektrum gefahrenabwehrender Maßnahmen" zu prüfen, und einige davon haben es in sich. „Den nationalen Gesetzgeber trifft die verfassungsrechtliche Pflicht, die Demokratie vor den Gefahren für die freie demokratische und plurale Meinungsbildung, die von Anbietern mit Torwächterfunktion ausgehen, durch Etablierung einer positiven Medienordnung zu schützen", steht dazu im Gutachten. Plattformen sollten dazu verpflichtet werden, ihren Nutzerinnen und Nutzern auch eine tendenzfreie und ausgewogene Zusammenstellung von Informationen zu bieten. Sollte dies umgesetzt werden, müssten etwa Facebook oder YouTube allen NutzerInnen die Option einräumen, den personalisierten Feed abzuschalten.

Aufsicht über Datenschutz an einer Stelle bündeln

Auch in Hinblick auf die Erhebung und Verarbeitung personenbezogener Daten fordert die Kommission eine „Konkretisierung und punktuelle Verschärfung des Rechtsrahmens". So diagnostiziert sie eine eklatante Durchsetzungslücke beim Datenschutz. Dem müsse unter anderem durch mehr Personal und Geld für die Aufsichtsbehörden begegnet werden.

Die Kommission bringt zudem die Idee ins Spiel, die Aufsichtskompetenz über die Wirtschaft – derzeit auf 16 Landes- und eine Bundesbehörde verteilt – an einer Stelle zu bündeln. Mangelhafte Abstimmung habe in der Vergangenheit bisweilen zu unterschiedlichen Rechtsaussagen der Behörden geführt. Mindestens müsse daher ihre Abstimmung untereinander verbessert werden. Im Gremium sitzt auch der Bundesdatenschutzbeauftragte Ulrich Kelber, der diese Idee schon öfter ins Spiel brachte.

Schärfere Regeln fordert die Kommission etwa im Fall von Profilbildungen und Scoring, „um den Gefahren der Manipulation und der Diskriminierung des Einzelnen wirkungsvoll begegnen zu können". Bei diesen Verfahren werden personenbezogene Daten zusammengeführt und genutzt, um Eigenschaften von Menschen zu prognostizieren und sie zu bewerten, etwa durch Auskunfteien wie die Schufa.

Weil es durchaus gewünschte Formen des datengetriebenen Profilings gebe, spricht sich das Gutachten gegen ein grundsätzliches Verbot aus. Allerdings sollten bestimmte Einsatzzwecke sowie Profilbildung mit sensiblen Daten untersagt und bindende Qualitätsstandards festgeschrieben werden. Bestenfalls sei dies durch eine Ergänzung der Datenschutzgrundverordnung zu erreichen, auf die die Bundesregierung im Rahmen der 2020 anstehenden Evaluation hinwirken sollte.

Außerdem betont die Kommission, dass Geschäftspraktiken von Digitalkonzernen, die auf Irreführung oder Manipulation beruhen, unabhängig von Datenschutzvergehen schon heute verboten seien. So seien so genannte Addictive Designs und Dark Patterns, bei denen Benutzeroberflächen gezielt so gestaltet werden, dass sie Sucht erzeugen oder NutzerInnen zur Auswahl gewünschter Optionen (etwa schwache Datenschutzeinstellungen) lenken, als „irreführendes oder aggressives Verhalten nach dem Gesetz gegen den unlauteren Wettbewerb (UWG)" zu verstehen.

Eigentumsrecht löst das Problem nicht

Eine deutliche Abfuhr erteilt die Kommission der Idee eines neu zu schaffenden Eigentumsrechts an Daten. Bundeskanzlerin Angela Merkel hatte vor einiger Zeit gemeinsam mit dem damaligen Verkehrsminister Alexander Dobrindt für die Idee geworben, damit Unternehmen einfacher mit Daten als Handelswaren arbeiten können. Verbraucher- und Datenschutzorganisationen hatten davor gewarnt, weil es dazu führen könnte, Menschen zu entmündigen. Nun hält auch das Gutachten fest, ein Eigentumsrecht an Daten würde „bestehende Probleme nicht lösen", aber insbesondere Einkommensschwache und Minderjährige zur Preisgabe möglichst vieler Daten verführen.

Während die Kommission also einen deutlich besseren Schutz personenbezogener Daten fordert, betont sie das Potenzial von Daten für das Gemeinwohl. Insbesondere im Gesundheitsbereich und in der Forschung müsse die Rechtslage dafür aber klarer werden. Außerdem müsse die Bundesregierung ihre Anstrengungen verstärken, Standards und Verfahren zur Anonymisierung und Pseudonymisierung personenbezogener Daten zu etablieren. Flankiert werden sollte dies von einem Verbot, Anonymisierungen und Pseudonymisierungen rückgängig zu machen.

Außerdem schlägt sie eine bundesweite Vereinheitlichung der Rechtslage im Bereich Open Data und eine gesetzliche Bereitstellungspflicht für Behördendaten (*Open by Default*) vor, inklusive dem Recht, dies individuell einzuklagen.

Die Kommission als Joker

Die Datenethikkommission wurde im Herbst 2018 von der damaligen Bundesjustizministerin Katarina Barley (SPD) und Bundesinnenminister Horst Seehofer (CSU) berufen. Sie sollte „ethische Leitplanken" für den Umgang mit algorithmischen Systemen und Daten entwickeln und Antworten liefern, um die Rechte von BürgerInnen zu stärken – egal ob diese nun einem Unternehmen oder dem Staat gegenüber stehen. Ein Jahr hatten die Rechtswissenschaftler, Ethikerinnen, Verbraucherschützer und Wirtschaftsvertreter Zeit, um sich auf die jetzt vorgestellten Empfehlungen zu einigen.

Der Rechtswissenschaftler Mario Martini, der an den Regulierungsbausteinen gearbeitet hat, wiegelt das Ergebnis ab. „Letztlich haben wir nichts Neues erfunden", sagt er. Alle Empfehlungen stützten sich alle auf Expertisen, die bereits anderswo nachzulesen seien. Mag sein. Dass sie nun in einem Dokument stehen, das der Bundesregierung als Empfehlung vorliegt, macht sie dennoch explosiver. Das erkennt man schon an der Aufregung von wirtschaftsnahen Medien, die eine neue „Regulierungswelle" heranrollen sehen[8].

Im vergangenen Jahr war die Datenethikkommission der Joker, den die Bundesregierung jedes Mal aus dem Ärmel ziehen konnte, wenn kritische Fragen gestellt wurden. Egal, ob in der Strategie Künstliche Intelligenz[9] oder bei Podiumsdiskussionen mit der Kanzlerin, stets hieß es: „Wir haben da diese Kommission." Diese Ausrede ist nun hinfällig. Der Ball liegt wieder bei den PolitikerInnen. Sie werden sich ranhalten müssen. In der EU-Kommission arbeitet man bereits an Entwürfen für eine neue Algorithmen-Verordnung.

Quelle: https://netzpolitik.org/2019/regierungsberaterinnen-fordern-strengere-regeln-fuer-daten-und-algorithmen/

Anmerkungen

1 *https://datenethikkommission.de/gutachten/*
2 *23. Oktober 2019*
3 *https://netzpolitik.org/2019/200-seiten-erwartungsdruck/*
4 *https://netzpolitik.org/2019/firmen-verleihen-sich-selbst-ein-guetesiegel-fuer-kuenstliche-intelligenz/*
5 *https://netzpolitik.org/2019/keine-roten-linien-industrie-entschaerft-ethik-leitlinien-fuer-kuenstliche-intelligenz/*
6 *https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/themen/it-digitalpolitik/datenethikkommission/leitfragen-datenethikkommission.pdf?__blob=publicationFile&v=1*
7 *https://twitter.com/algorithmwatch/status/1137298220760125440*
8 *https://www.faz.net/aktuell/wirtschaft/diginomics/neue-daten-regulierungswelle-rollt-an-16445772.html*
9 *https://netzpolitik.org/2019/in-diese-projekte-fliesst-das-geld-das-die-regierung-zur-ki-foerderung-ausgibt/*

Ingo Dachwitz und Chris Köver

200 Seiten Erwartungsdruck

Kommentar zur Datenethikkommission

Die Datenethikkommission hatte alle Voraussetzungen um zu scheitern. Stattdessen hat sie der Regierung eine Liste vorgelegt, die weit über bisherige Empfehlungen hinausgehen. Nun muss die Große Koalition zeigen, dass dieses Gutachten nicht nur für die Schublade war. Ein Kommentar.

16 Mitglieder, die Hälfte davon Frauen, und ein Jahr Zeit. Selten hatte ein Gremium ein solches symbolisches Päckchen zu tragen wie die Datenethikkommission der Bundesregierung. Im Grunde muss man von einer Last sprechen. Egal, ob in der Strategie Künstliche Intelligenz oder bei kritischen Nachfragen zu Konsequenzen aus dem Cambridge-Analytica-Skandal: stets musste die Kommission als Joker herhalten.

Nicht weniger als die Grundlage für ein „neues Datenrecht“[1] solle sie schaffen, versprach Kanzleramtsminister Helge Braun. Heute hat die Kommission ihr Abschlussgutachten vorgelegt. [Lest hier auch unsere Zusammenfassung des Gutachtens der Datenethikkommission: RegierungsberaterInnen fordern strengere Regeln für Daten und Algorithmen[2]; siehe Seite 46.]

Kommission statt Vision

Wie sie denn mit dem enormen Erwartungsdruck umgehen würden, hatten wir die Vorsitzenden im Mai 2019 auf der re:publica gefragt. Ihre charmante Antwort: „Mit Verdrängung“[3]. Was sollten sie auch sagen? Statt nach der Bundestagswahl 2017 Richtungsentscheidungen in der Daten- und Algorithmenpolitik[4] zu treffen, vertagten CDU, CSU und SPD die Auseinandersetzung.

Die Unionsparteien hatten in ihrem Wahlprogramm Angela Merkels Mantra von „Daten als Rohstoff der Zukunft“ folgend ein Datengesetz angekündet, das Wirtschaft und Behörden den Zugriff auf Daten erleichtern sollte. Auch die SPD betonte das wirtschaftliche Potenzial von Daten, kündigte aber diverse Maßnahmen zum Schutz von VerbraucherInnen an, etwa einen „Algorithmen-TÜV“ und strengere Regeln für Risikoscoring.

Statt gemeinsamer Visionen setzte man also auf eine neue Kommission – typisch GroKo eben. Sie sollte „einen Entwicklungsrahmen für Datenpolitik, den Umgang mit Algorithmen, künstlicher Intelligenz und digitalen Innovationen“ erarbeiten, hieß es im Koalitionsvertrag. Die Ergebnisse sollten dann „Geschwindigkeit in die digitale Entwicklung bringen und auch einen Weg definieren, der gesellschaftliche Konflikte im Bereich der Datenpolitik auflöst“.

Meinungsmanipulation? Die Erde ist doch keine Kugel

Das neue Datenrecht ist das alte

Wie machen sich die Ergebnisse nun also im Vergleich zu diesen hoch gesteckten Zielen? Hinter vorgehaltener Hand – die Kommission entschied sich dafür, das fast 200 Seiten starke Gutachten vorab nicht mal der Presse zur Verfügung zu stellen – ließen manche Mitglieder bereits durchblicken: Der große Wurf wird es nicht. Wie sollte das innerhalb eines Jahres bei diesem breiten Themenzuschnitt auch gehen?

Und doch: Nach einer ersten Lektüre kann man sagen, dass das Gutachten durchaus wegweisend ist. Verständlich beschrieben und mit praktischen Beispielen untermauert, seziert es aktuelle Probleme und enthält sehr viele Vorschläge für konkrete Gegenmaßnahmen. Von denen könnte die Bundesregierung einige sofort umsetzen, viele müsste sie auf europäischer Ebene anstoßen.

Grob zusammengefasst sagt die Kommission: Das „neue Datenrecht“ sollte das alte sein – nur besser durchgesetzt und in

Chris Köver und Ingo Dachwitz

Chris Köver berichtet für *netzpolitik.org* über maschinelles Lernen, Digitale Gewalt und die Verletzungen der Grundrechte von Frauen, Geflüchteten und anderen marginalisierten Gruppen. Außerdem ist sie eine der Moderatorinnen des wöchentlichen *netzpolitik.org-Podcasts*. Chris ist eine der Gründerinnen des *Missy Magazine* und hat acht Jahre lang als Chefredakteurin das Magazin zum feministischen Zentralorgan aufgebaut. Sie gibt Schreib-Workshops an Journalistenschulen und Universitäten und hat zwei Sachbücher veröffentlicht. Kontakt: E-Mail[5], OpenPGP[6], Twitter[7].

Ingo Dachwitz siehe Seite 53.

einigen Punkten konkretisiert und verschärft. Zumindest, was den Bereich der personenbezogenen Daten angeht. Gleichzeitig sollte die Bundesregierung mehr dafür tun, dass öffentliche Daten von allen genutzt werden können, und dass Medizin und Forschung einen sicheren Rahmen haben, um mit Daten am Gemeinwohl zu arbeiten.

In Sachen algorithmischer Systeme geht das Gutachten weit über bisherige Empfehlungen hinaus. In einigen Teilen bleibt es vage, etwa bei der Frage, wie die algorithmengesteuerten Feeds von Social-Media-Plattformen und die Gefahr der Meinungsmanipulation eingehegt werden könnten. An anderen Stellen werden die Empfehlungen jedoch derart konkret, dass sie sich wie ein Handbuch für die Regierung lesen: „Richtig regieren im Informationszeitalter". Noch deutlicher hätte das Gremium nur noch werden können, hätte es als Anhang gleich den Gesetzestext mitgeliefert. Das ist aber natürlich nicht die Aufgabe von Fachleuten, das müssen jene machen, die für den Job gewählt wurden.

Eine Frage des politischen Willens

Vieles von dem, was die Kommission empfiehlt, steht im Widerspruch zur ausschließlich marktorientierten Daten- und Algorithmenpolitik gerade der Unionsparteien. Dass CDU und CSU in Reaktion auf das Gutachten ihre politische Linie aufgeben, dürfte unwahrscheinlich sein. Genau so unwahrscheinlich ist es, dass die SPD die Kraft aufbringt, die empfohlenen Maßnahmen durchzusetzen.

Es wäre nicht das erste aufwendig erarbeitete netzpolitische Gutachten, dass die Bundesregierung im Schreibtisch verschwinden lässt. Das führt uns also wieder an den Ursprung des Problems: den fehlenden politischen Gestaltungswillen einer Großen Koalition, die nur deshalb noch zusammen hält, weil alle Beteiligten Angst vor Neuwahlen haben.

Wissenschaft und Zivilgesellschaft sollten das Gutachten künftig trotzdem als Maßstab nehmen, an dem sie die Digitalpolitik der Bundesregierung messen.

Quelle: https://netzpolitik.org/2019/200-seiten-erwartungsdruck

Anmerkungen

1 *https://www.faz.net/aktuell/wirtschaft/diginomics/kanzleramtschef-helge-braun-kuendigt-neues-datenrecht-an-15507255.html*
2 *https://netzpolitik.org/2019/regierungsberaterinnen-fordern-strengere-regeln-fuer-daten-und-algorithmen/*
3 *https://re-publica.com/en/session/weiter-datenpolitik*
4 *https://netzpolitik.org/2017/der-netzpolitische-wahlprogramm-vergleich-teil-9-verbraucherschutz-und-digitale-souveraenitaet/*
5 *chris@netzpolitik.org*
6 *https://sks-keyservers.net/pks/lookup?op=get&search=0x5E598DD0D37B9F71A88DD92233D38859243016F9*
7 *http://www.twitter.com/ckoever*

Markus Beckedahl und Ingo Dachwitz

Überfälliger Wegweiser für die einen, Innovationsbremse für die anderen

Reaktionen auf die Datenethikkommission

Wir haben Reaktionen auf den Abschlussbericht der Datenethikkommission gesammelt. Während Bundesregierung und Zivilgesellschaft positiv auf die Ergebnisse reagieren, warnen Lobbyverbände der Industrie vor „Regulierungswut". Im Bundestag fällt das Echo positiv bis ambivalent aus.

Mittwoch hat die Datenethikkommission der Bundesregierung ihr Abschlussgutachten[1] vorgelegt. Die Kommission wurde vor einem Jahr gemeinsam vom Bundesinnenministerium und dem Justizministerium eingerichtet, um Antworten auf einige der kniffeligsten Fragen zum Umgang mit Daten und Algorithmen zu liefern und ethische Leitplanken zu definieren. Unsere erste Analyse zeigt: Das ist besser gelungen, als wir erwartet hatten[2].

Der Bundesministerin für Justiz und Verbraucherschutz, Christine Lambrecht[3], liegt einer ersten Äußerung zufolge „viel daran, dass wir gemeinsam eine wertebasierte, menschenzentrierte und gemeinwohlorientierte digitale Zukunft gestalten, die niemanden zurücklässt und der die Menschen vertrauen können." Sie ist froh, „dass die Datenethikkommission sowohl ethische Leitlinien als auch konkrete rechtliche Handlungsempfehlungen" vorgelegt hat. Sie will die Empfehlungen der Datenethikkommission „nun im Detail auswerten und bei unserem politischen Handeln berücksichtigen."

Der Parlamentarische Staatssekretär Günter Krings aus dem Bundesinnenministerium möchte[4], dass die Bürgerinnen und Bürger „den digitalen Wandel mitgestalten", „um selbstbestimmt mit den Risiken umgehen zu können". Die Ergebnisse der Kommission würden „hierfür einen wichtigen Beitrag" leisten.

„Steilvorlage für die Zivilgesellschaft"

Klaus Müller, Vorstand des Verbraucherzentrale Bundesverband und Mitglied der Datenethikkommission sieht die Bundesregierung am Zug[5] und wünscht sich, dass sie die Empfehlungen „so schnell wie möglich" umsetze.

Lorenz Matzat hat für Algorithmwatch[6] eine kurze Analyse geschrieben und beurteilt die Empfehlungen als „eine überfällige und substanzielle Diskussionsgrundlage" und als „Steilvorlage für die Zivilgesellschaft". Auch wenn er einige kritische Fragen hat: An dem Gutachten werde „man zumindest in Deutschland

im Diskurs über den Umgang mit Daten (auch jenseits des Datenschutzes) sowie automatische Entscheidungen nicht mehr vorbeikommen."

Auch der TÜV-Verband[7] begrüßt das Gutachten. Der Präsident der Prüfstellen-Vereinigung, Joachim Bühler, sieht „in unabhängigen Prüfungen Künstlicher Intelligenz zur Sicherheit von Verbrauchern, Beschäftigten und Unternehmen ein Instrument, um KI-Innovationen auf dem europäischen Markt zum Durchbruch zu verhelfen."

Industrie: Ethik schön und gut, aber bitte ohne Konsequenzen!

Der Industrieverband Bitkom begrüßt zwar[8], „dass wir in Deutschland einen breiten gesellschaftlichen Dialog über Datenethik führen." Aber das war es auch schon mit Lob. Anstatt über Risiken möchte man lieber über Chancen reden und sieht in Transparenz mehr Chancen als in echten Verbraucherrechten. Nicht fehlen darf die Warnung vor „Regulierungswut". Das geht dann so weit, dass Bitkom-Präsident Achim Berg vor einem Rückbau Deutschlands „zu einem analogen Inselstaat" warnt.

Wenig überraschend findet auch eco, der Verband der Internetwirtschaft[9]: Ethik schön und gut, aber bitte ohne zu stören. Die Organisation „warnt vor Unmengen neuer Gesetze und Regeln" und „blinder Überregulierung", denn die „würde die Entwicklung und den Einsatz von Künstlicher Intelligenz als Schlüsseltechnologie massiv beeinträchtigen und die Digitalisierung in Deutschland nur noch weiter verzögern."

Ähnlich klingt es auch beim Verband Deutscher Maschinenbauer[10]. Dessen Geschäftsführer Software und Digitalisierung, Claus Oetter, beklagt: „Überbordende Regulierungen blockieren die technologischen Innovationen sowie eine dynamische Marktentwicklung, das darf nicht passieren. Datenethik ist wichtig, doch sie muss für die Industrie praxistauglich sein und darf keine voreiligen Grenzen ziehen. Nur dann kann künstliche Intelligenz einen wichtigen Beitrag zu einer fortschrittlichen technologischen Entwicklung leisten.

CDU wiegelt ab, Linke lobt, SPD schweigt

Im Ton etwas zurückhaltender – immerhin hat die eigene Regierung das Gutachten in Auftrag gegeben –, in der Sache aber äußerst ähnlich wie bei den Wirtschaftsverbänden, klingt es bei der CDU/CSU-Bundestagsfraktion[11]. In deren Namen warnen die Abgeordneten Nadine Schön und Tankred Schipanski vor einer Überforderung des Marktes, wollen aber die „Vielzahl vorgeschlagener Maßnahmen" nun umfassend prüfen und „uns dabei an den Chancen orientieren".

Die beiden linken Bundestagsabgeordneten Anke Domscheit-Berg und Petra Sitte[12] begrüßen, „dass die Datenethikkommission weitgehende Vorschläge zur Algorithmenregulierung vorgelegt hat und nun eine umfassende Diskussionsgrundlage bietet."

Aus der Grünen Bundestagsfraktion[13] melden sich Tabea Rösner und Konstantin von Notz zu Wort. Sie sehen sich durch die Empfehlungen der Kommission in vielen Punkt bestätigt und nutzen die Gelegenheit für einen Angriff auf die Bundesregierung: „Wie zuvor die Expertenkommission zum Wettbewerbsrecht nimmt auch die Datenethikkommission die offenkundig überforderte Bundesregierung mit der Vorlage ihrer ebenso klaren wie zukunftsfähigen Handlungsempfehlungen in zentralen Zukunftsfragen an die Hand. Sie macht deutlich, dass Regulierung alles andere als Teufelswerk ist, sondern Verbraucherrechte sichert, Diskriminierung verhindert und Unternehmen dringend benötigte Rechtssicherheit bietet."

Der technologiepolitische Sprecher der FDP-Fraktion im Bundestag[14], Mario Brandenburg, hat sowohl Lob als auch Kritik für das Gutachten. Die Datenethikkommission schüre Ängste, findet der Wirtschaftsinformatiker. Dass bestimmte algorithmische Systeme vor ihrer Markteinführung geprüft werden sollen, gefährde einen „First Mover Advantage" und Deutschlands internationale Wettbewerbsfähigkeit. Gleichwohl hält er fest: „Viele Punkte, wie Privacy-by-Design, Interoperabilität, Explainable AI oder das Einschalten von „Datentreuhändern", um die Kooperation auf europäischer Ebene voranzutreiben und Bürgerrechte zu schützen, begrüßen wir Freie Demokraten."

Eine Stellungnahme der SPD-Fraktion oder ihrer NetzpolitikerInnen konnten wir bisher nicht finden.

Markus Beckedahl und Ingo Dachwitz

Markus Beckedahl ist Gründer und Chefredakteur von *netzpolitik.org*. Er ist Partner bei *newthinking communications GmbH*[17], Gründer der *re:publica*[18] 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[19] / Twitter: *@netzpolitik* / Instagram: *@netzpolitik* / Amazon: Die Wunschliste[20] von Markus.

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 manchmal an Universitäten zur politischen Ökonomie digitaler Medien. Gelegentlich moderiert er auch Veranstaltungen und Diskussionen, etwa auf der re:publica oder beim Netzpolitischen Abend in Berlin. Ingo ist Mitglied der sozialethischen Kammer der EKD und berät kirchliche Organisationen bei der digitalen Transformation.
Kontakt: Ingo ist per Mail an ingo | ett | netzpolitik.org (PGP-Key[21]) erreichbar und als *@roofjoke* auf Twitter unterwegs.

Maßstab für die künftige Digitalpolitik

Chris Köver und Ingo Dachwitz kommentierten bei uns[15]: „Nach einer ersten Lektüre kann man sagen, dass das Gutachten durchaus wegweisend ist. Verständlich beschrieben und mit praktischen Beispielen untermauert, seziert es aktuelle Probleme und enthält sehr viele Vorschläge für konkrete Gegenmaßnahmen. Von denen könnte die Bundesregierung einige sofort umsetzen, viele müsste sie auf europäischer Ebene anstoßen. […] Wissenschaft und Zivilgesellschaft sollten das Gutachten künftig als Maßstab nehmen, an dem sie die Digitalpolitik der Bundesregierung messen."

Update: Hinter der Paywall vom Handelsblatt haben wir doch noch eine Äußerung eines SPD-Abgeordneten[16] gefunden. Jens Zimmermann ist netzpolitischer Sprecher der Bundestagsfraktion: „Den Einsatz von Algorithmen per se zu verbieten, wird in der digitalen Welt nicht möglich sein", sagte der Bundestagsabgeordnete dem Handelsblatt. „Wir wollen den technischen Fortschritt." Gleichwohl dürfe der Einsatz der Algorithmen nicht zur Diskriminierung und weiteren Kartellbildung in der digitalen Welt führen. „Die Machtkonzentration muss aufgebrochen werden und zwar mit klaren Regeln für Transparenz und Offenlegung", sagte Zimmermann.

Quelle: https://netzpolitik.org/2019/ueberfaelliger-wegweiser-fuer-die-einen-innovationsbremse-fuer-die-anderen

Anmerkungen

1 *https://datenethikkommission.de/gutachten/*
2 *https://netzpolitik.org/2019/regierungsberaterinnen-fordern-strengere-regeln-fuer-daten-und-algorithmen/*
3 *https://www.bmjv.de/SharedDocs/Artikel/DE/2019/102419_Abschlussbericht_DEK.html*
4 *https://www.bmi.bund.de/SharedDocs/kurzmeldungen/DE/2019/10/datenethikkommission.html*
5 *https://www.vzbv.de/pressemitteilung/algorithmen-abschied-nehmen-von-der-blackbox*
6 *https://algorithmwatch.org/bericht-der-datenethikkommission-steilvorlage-fuer-die-zivilgesellschaft/*
7 *https://www.datensicherheit.de/aktuelles/vdtuev-begruesst-abschlussbericht-der-datenethikkommission-35018*
8 *https://bitkom.de/Presse/Presseinformation/Bitkom-Abschlussbericht-Datenethikkommission*
9 *https://www.eco.de/presse/eco-kommentiert-abschlussbericht-der-datenethikkommission-regulierungsphantasien-werden-zur-digitalisierungs-bremse/*
10 *https://www.vdi-nachrichten.com/technik/vdma-gleichbehandlung-von-b2b-und-b2c-nicht-zielfuehrend/*
11 *https://www.cducsu.de/presse/pressemitteilungen/neue-wege-beim-datenschutz-gehen*
12 *https://www.linksfraktion.de/presse/pressemitteilungen/detail/bundesregierung-muss-sich-mit-empfehlungen-der-datenethikkommission-auseinandersetzen/*
13 *https://gruen-digital.de/2019/10/bundesregierung-muss-vorschlaege-der-datenethikkommission-zuegig-umsetzen/*
14 *https://mbrandenburg.abgeordnete.fdpbt.de/meldung/Gutachten-Datenethikkommission*
15 *https://netzpolitik.org/2019/200-seiten-erwartungsdruck/*
16 *https://www.handelsblatt.com/politik/deutschland/bericht-der-datenethikkommission-regierungskommission-loest-debatte-ueber-algorithmen-regulierung-aus/25146582.html*
17 *http://newthinking.de/*
18 *http://re-publica.de/*
19 *https://www.facebook.com/beckedahl*
20 *http://www.amazon.de/gp/registry/wishlist/279FWSUX7VB9*
21 *https://pgp.mit.edu/pks/lookup?op=get&search=0x05550760A5E4E814*

Matthias Monroy

NATO errichtet Biometriedatenbank nach Vorbild der USA

Das US-Verteidigungsministerium speichert Millionen Menschen mit Gesicht, Iris, Fingerabdrücken und DNA, eine dazugehörige Warndatei ist mit Polizeibehörden vernetzt. Die NATO will ein ähnliches System aufbauen. In weitaus größerem Umfang sammeln allerdings Flüchtlingsorganisationen biometrische Daten von Schutzsuchenden.

Das Militär der Vereinigten Staaten verfügt über eine Datenbank mit Millionen Gesichtsbildern, Iris-Fotos, Fingerabdrücken und DNA-Daten. In diesem *Automated Biometric Information System* (ABIS) sind derzeit 7,4 Millionen Identitäten gespeichert, berichtet das Nachrichtenmagazin *OneZero*[1]. Die Angaben stammen aus einer Anfrage nach dem Informationsfreiheitsgesetz und basieren auf der Präsentation eines Mitarbeiters im Verteidigungsministerium.

Die militärische Biometrieagentur verwaltet die Datei. Gesammelt werden Daten in Ländern, in denen das US-Militär aktiv ist. Das System soll Terrorverdächtige und deren Kontaktpersonen identifizieren und aufspüren, biometrische Spuren werden unter anderem von gefangenen oder getöteten GegnerInnen abgenommen. Daten stammen laut OneZero aber auch aus Wählerregistrierungen, Arbeitsverhältnissen oder sonstigen Informationen, an die das Militär gelangt. Auch verbündete SoldatInnen werden erfasst.

Weltweit vernetzte Warndatei

Das ABIS ermöglicht außerdem, einzelne Personen in eine sogenannte *Biometrically Enabled Watch List* (BEWL) einzutragen. Die Warndatei kann mit Systemen von Polizeien oder Geheimdiensten verbunden werden und gibt einen Alarm aus, wenn die Betroffenen eine Grenze passieren oder in eine Polizeikontrolle geraten. Dieses System ist auch über mobile Geräte zum Abgleich von Fingerabdrücken, Iriden oder Gesichtern nutzbar.

Derzeit sollen mehr als 213.000 Personen in der BEWL gespeichert sein. Im ersten Halbjahr 2019 wurden laut der Präsentation des US-Verteidigungsministeriums 4.467 Treffer mithilfe der Warndatei erzielt, davon waren etwa zwei Drittel gegnerische Kräfte in Kriegsgebieten.

Dem Bericht zufolge ist das ABIS unter anderem mit der biometrischen Datenbank des FBI verbunden, die an weitere lokale Polizeidatenbanken angeschlossen ist. US-Behörden arbeiten demnach auch an einer Vernetzung mit der Biometriedatenbank des Heimatschutzministeriums. Auf diese Weise könnte das ABIS zu einem weltweiten zivil-militärischen Informationssystem ausgebaut werden. Auch europäische Polizei- und Geheimdienstbehörden fragen biometrische Daten beim den zuständigen Polizeibehörden und dem US-Militär ab.

NATO-System ohne DNA-Daten?

Vor einem Jahr haben auch die NATO-Mitgliedstaaten den Aufbau einer Biometriedatenbank beschlossen[2]. Unter dem Namen *NATO Automated Biometric Identification System* (NABIS) sollen dort Daten zu Gesicht, Iris und Finger gespeichert werden. Das deutsche Verteidigungsministerium bestätigt die Angaben[3], erwähnt aber keine DNA-Daten.

Zwar ist das System nach offiziellen Angaben noch in der Entwicklung, ein Prototyp wurde der NATO zufolge[4] jedoch schon im Jahr 2014 im gemeinsamen Manöver *Unified Vision* getestet. In einem Papier[5] hat das US-Militär die damaligen technischen Spezifikationen des ABIS erklärt.

In einer späteren Version könnten auch Hände und Venen, Handschriften, Sprechproben, Tastendruck oder der Gang von Personen als biometrische Informationen erhoben und verarbeitet werden. Für die NATO und die mit dem Bündnis verbundenen Truppen sind diese Daten von grundlegendem Interesse[6].

Anbindung internationaler Polizeiorganisationen

Derzeit ist nicht bekannt, welche Hersteller mit der Entwicklung des NABIS beauftragt sind. Zuständig für das Projekt ist die Kommunikations- und Informationsagentur der NATO[7] mit Sitz in Den Haag. Es ist denkbar, dass das NABIS auf dem ABIS des US-Militärs aufbaut oder dessen technische Infrastruktur nutzt. Laut OneZero wird das US-System von dem amerikanischen Konzern Leidos errichtet, der hierfür 150 Millionen Dollar erhielt und weitere US-Firmen als Auftragnehmer verpflichtet.

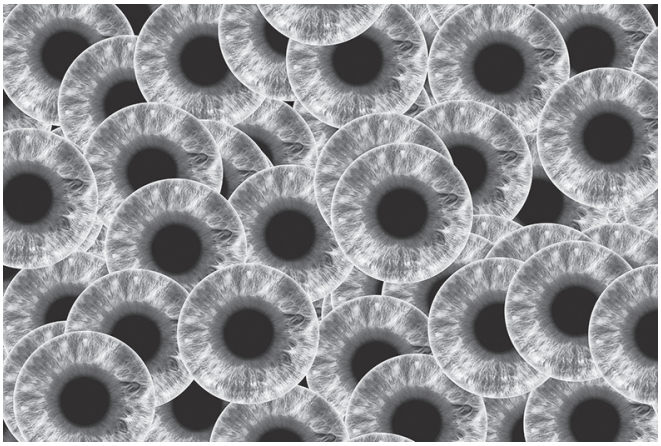


Bild: Hebi B. auf Pixabay

Für eine Datenbank in Afghanistan ist demnach die Firma Ideal Innovations Incorporated verantwortlich. Dabei handelt es sich vermutlich um das System HAMAH, eine ähnliche Datensammlung zu „Daten von Kriegsschauplätzen" (*battlefield data* oder *battlefield information*) betreibt das US-Militär unter dem Namen VENLIG im Irak. Auch die Polizeiagentur Europol sowie Interpol werden vom US-Militär in die beiden Systeme eingebunden und liefern bei Bedarf Daten zu gespeicherten Personen. Werden „Bezüge zu Deutschland festgestellt", erfolgt laut der Bundesregierung[8] auch eine Anfrage an das Bundeskriminalamt (BKA) über dort vorhandene Informationen.

HAMAH und VENLIG dürften die Vorläufer der neuen US-Biometrie-Datei gewesen sein, jedenfalls schreibt OneZero, dass die meisten der sieben Millionen Identitäten aus Afghanistan und dem Irak stammen. Auch in der Operation *Gallant Phoenix*[9] sammelt das US-Militär biometrische Daten in Syrien und dem Irak. Aus EU-Dokumenten ergibt sich, dass daran auch Europol beteiligt ist, aus Deutschland außerdem der Bundesnachrichtendienst[10].

UN-Flüchtlingskommissar betreibt eigenes System

Neben Militär, Geheimdiensten und Polizei sammeln auch Hilfsorganisationen in großem Umfang biometrische Daten. Der Hohe Flüchtlingskommissar der Vereinten Nationen (UNHCR) betreibt in 66 Ländern ein System zur Identifikation, Registrierung und Verwaltung von Schutzsuchenden. In diesem *Biometric Identity Management System* werden auch Kinder ab fünf Jahren mit Gesichtsfoto, Fingerabdrücken beider Hände und Bildern beider Irides erfasst.

Das Biometriesystem des UNHCR wird zentral geführt und in Gebieten ohne Internet auf lokalen Servern gespiegelt. Ihr

Matthias Monroy

Matthias Monroy[13], Wissensarbeiter, Aktivist und Mitglied der Redaktion der Zeitschrift Bürgerrechte & Polizei/CILIP[14]. 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.*

Standort ist aus Sicherheitsgründen geheim. Für das Scannen von Iris und Fingerabdrücken wird unter anderem Software von den Firmen Accenture, Greenbit und IriTech genutzt. Nach Angaben des Auswärtigen Amtes[11] liegen derzeit 8,2 Millionen Erwachsene und Kinder in der Datei. In einem ähnlichen des Welternährungsprogramms der Vereinten Nationen sind demnach biometrische Informationen zu 11,4 Millionen Begünstigten aus 32 Ländern gespeichert.

Über Umwege können die Informationen zu Geflüchteten auch in den polizeilichen oder militärischen Biometriedateien landen. Unter „angemessenen Umständen", etwa wenn gegen Personen ermittelt wird[12] oder diese (mit ihrer Zustimmung) als ZeugInnen aussagen sollen, übermittelt das UNHCR personenbezogene Daten an Strafverfolgungsbehörden oder Gerichte. Dies geschieht auf Anfrage der Behörden oder auch auf eigene Initiative des UNHCR. Die Weitergabe kann auch zur Gefahrenabwehr erfolgen, etwa um Straftaten oder eine Gefährdung der öffentlichen Sicherheit zu verhindern. Die Behörden sollen aber versichern, dass die Daten nicht anderweitig verwendet werden.

Quelle: https://netzpolitik.org/2019/nato-errichtet-biometrie-datenbank-nach-vorbild-der-usa/

Anmerkungen

1 *https://onezero.medium.com/exclusive-this-is-how-the-u-s-militarys-massive-facial-recognition-system-works-bb764291b96d*
2 *https://www.nato.int/cps/en/natohq/official_texts_156624.htm*
3 *http://dipbt.bundestag.de/doc/btd/19/136/1913673.pdf*
4 *https://www.nato.int/cps/en/natohq/news_117917.htm?selectedLocale=en*
5 *https://www.marines.mil/Portals/1/MCRP%203-33.1J%20BIOMETRICS%201.pdf*
6 *http://www.jwc.nato.int/images/stories/threeswords/Biometrics_2018.pdf*
7 *https://www.ncia.nato.int/Pages/homepage.aspx*
8 *https://dipbt.bundestag.de/dip21/btd/18/014/1801411.pdf*
9 *https://netzpolitik.org/2017/europol-startet-datentauschring-mit-geheimdiensten-und-us-militaer/*
10 *https://www.wn.de/Welt/Politik/3157871-Operation-Gallant-Phoenix-Bericht-BND-beteiligt-sich-an-US-Geheimaktion-gegen-IS*
11 *https://www.andrej-hunko.de/start/download/dokumente/1411-sammlung-und-verarbeitung-biometrischer-daten-in-hilfsprogrammen-der-vereinten-nationen/file*
12 *https://www.refworld.org/docid/55643c1d4.html*
13 *https://netzpolitik.org/author/matthias/*
14 *http://www.cilip.de/*

Lesen & Sehen

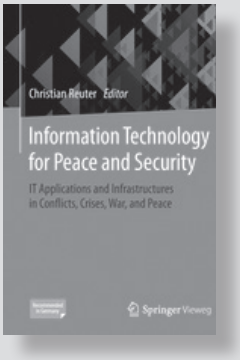
Neues für Bücherwürmer & Cineasten

Stefan Hügel

Christian Reuter (Editor): Information Technology for Peace and Security – IT Applications and Infrastructures in Conflicts, Crises, War and Peace

Der *Cyberspace* gilt längst als fünfte militärische Domäne, gleichrangig oder inzwischen sogar bedeutender als die klassischen militärischen Aktionsfelder Land, See, Luft und naher Weltraum. Der Cyberspace überschreitet physische, geografische und politische Grenzen. Er erfasst mittlerweile (fast) jeden Winkel dieser Erde und wird dadurch zum Ausspähraum gigantischen Ausmaßes. Und dennoch ist er paradoxerweise die letzte Domäne für verdeckte militärische Aktivitäten. Grund: Die Entwicklung und die Produktion von Waffen für Cyberoperationen benötigen keine auffälligen Anlagen; ihr Transport und ihre Stationierung erfordern keinen physischen Raum; ihre Erprobung und ihr Einsatz hinterlassen keine Spuren – zumindest keine physischen, und digitale Spuren können verdeckt, manipuliert oder sogar ausgelöscht werden.

Fragen des Friedens und der Sicherheit werden dadurch zum Anwendungsfeld der Informationstechnik. Damit sollten sie auch Inhalt der (akademischen) Lehre sein. Ihr Einfluss und ihre Nutzung in (kriegerischen) Konflikten ist Thema des hier besprochenen Bandes, der als Lehrbuch konzipiert und, so der Herausgeber, als Grundlage einer Vorlesung geeignet ist.



Christian Reuter *Editor* (2019)
Information Technology for Peace and Security – IT Applications and Infrastructures in Conflicts, Crises, War and Peace.
Wiesbaden: Springer Vieweg,
424 Seiten
Preis: 34,01 €uro
ISBN 978-3-658-25652-4,

Der Herausgeber, Professor am neu eingerichteten Lehrstuhl *Wissenschaft und Technik für Frieden und Sicherheit* (PEASEC) an der Technischen Universität Darmstadt, hat eine Reihe von Autorinnen und Autoren seines eigenen und weiterer Institute versammelt, deren Beiträge die Bedeutung, die Potenziale und die Herausforderungen der Informationstechnik für Frieden und Sicherheit behandeln, wie es im Vorwort heißt. Zu Beginn jedes Kapitels werden dessen Ziele formuliert; am Ende stehen eine

Zusammenfassung und Übungsaufgaben. Die Beiträge sind in Englisch abgefasst. Der Band umfasst 19 Kapitel in sieben Abschnitten von fast 30 Autorinnen und Autoren.

Der Abschnitt *Introduction and Fundamentals* gibt zunächst einen Überblick über die einzelnen Beiträge des Bandes. Danach wird die Rolle der Informationstechnologie (IT) in Friedens-, Konflikt und Sicherheitsforschung vertieft. Der Weg von der konventionellen Friedens- und Konfliktforschung zur technikbezogenen Friedensforschung wird gezeichnet und dabei die IT-Friedensforschung in der Schnittmenge zwischen technischer Friedensforschung und Cybersicherheit verortet. Zuletzt wird ein Überblick über die Forschungslandschaft in Deutschland (Forschungsinstitute und Nicht-Regierungsorganisationen) gegeben. Der letzte Beitrag des Abschnitts erörtert naturwissenschaftliche und technische Friedensforschung. Er geht auf das Sicherheitsdilemma ein, demzufolge verstärkte Sicherheitsbestrebungen letztlich zu mehr Unsicherheit führen. Er erläutert außerdem Maßnahmen zur Verminderung der militärischen Bedrohung (Rüstungskontrolle und verifizierte Abrüstung) und zur Erhöhung der Sicherheit (Nichtverbreitung und Exportkontrollen). Der Beitrag schließt mit Überlegungen, wie Informations- und Kommunikationstechnik sowie Forschung in diesem Feld den Frieden fördern können – wobei sie gleichzeitig eine zunehmende Rolle bei der Vorbereitung militärischer Konflikte spielen.

Der folgende Abschnitt befasst sich mit *Cyber Conflicts and War*. Der erste Beitrag dieses Buchteils zeichnet den Weg der Informationskriegführung von einer militärischen Doktrin zum alltäglichen Element eines permanenten Konflikts nach. Die Entwicklung zur primären Militärdoktrin begann in den 1990er Jahren, als zunächst die USA Konzepte für *Information Warfare* entwickelten: *command and control* gegen militärische Kommandostrukturen, *civil affairs operations* mit psychologischen Mitteln gegen die Zivilbevölkerung und *public affairs operations* als Public-Relations-Aktivitäten. Im weiteren Verlauf wurde Information Warfare weiter intensiviert und automatisiert und mündet heute in eine hybride Kriegführung, mit der man hybriden Bedrohungen durch reguläre Kräfte, irreguläre Kräfte, terroristische Angriffe und kriminelle Anteile begegnen will. Alle großen Mächte verfolgen heute solche Strategien und entwickel(te)n integrierte Waffensysteme auf der Basis von IT. Damit wurden Informationskriegführung und Cyberoperationen zum Mittel eines permanenten Konflikts zwischen staatlichen und nichtstaatlichen Akteuren.

Um Cyberspionage und Cyberabwehr geht es im folgenden Beitrag. Er grenzt Cyberspionage von traditionellen Formen der Spionage ab, führt in die Ziele der Informationssicherheit ein und stellt Designprinzipien für IT-Sicherheit, typische Angriffsszenarien durch die Ausnutzung von Schwachstellen und Abwehrmaßnahmen dar.

Der dritte Beitrag des Abschnitts geht auf die spezielle Bedeutung des Darknet für die Cyberkriegführung ein. Das Darknet ist ein Teil des Internet, in dem unbeobachtete, anonyme Kommunikation und die Vermeidung von Zensur, zumeist auf Basis des TOR-Netzwerks, möglich sein und damit die Attribuierung, d. h. die Zuordnung der Urheber von Transaktionen, weiter erschwert werden soll. Das Darknet wird mit seinen Risiken und Möglichkeiten vorgestellt. Im Rahmen der Cyberkriegführung wird es beispielsweise für den verdeckten Waffenhandel mit Cyberwaffen, für Destabilisierung, aber auch für zivilgesellschaftlichen Widerstand genutzt. Abschließend behandelt der Beitrag die *Versicherheitlichung*, d. h. die Transformation politischer Diskurse in Sicherheitsdiskurse, und verortet Cyberkriegführung und Darknets als deren Basis.

Ein Gegenkonzept zur Cyberkriegführung ist das im dritten Buchabschnitt erläuterte Konzept des *Cyber Peace*. Es geht von einer zunehmenden Militarisierung des Cyberspace aus und fragt nach Möglichkeiten für Sicherheit, Stabilität und Frieden angesichts des zunehmenden Fortschreitens der Militärtechnik. Daraus werden politische Schritte und Maßnahmen für eine friedenserhaltende Weiterentwicklung des Cyberspace abgeleitet. Grundprobleme sind die anonyme Nutzung von Cyberwaffen, deren mangelnde Kontrolle und dass sie uns mehr schaden als nützen. Beispielhaft werden bekannt gewordene Cyberattacken beschrieben, ebenso völkerrechtliche Initiativen, beispielsweise das *Tallinn Manual*, das völkerrechtliche Regeln und Normen für die Cyberkriegführung zusammenstellt. Schwierigkeiten der Rüstungskontrolle ergeben sich aus dem Konzept der *Aktiven Verteidigung* (z. B. durch Maßnahmen des *Hackback*) und Dual-use. Die *Cyberpeace*-Initiative des FIfF (Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung) mit dem dort entwickelten Forderungskatalog ist ein zivilgesellschaftlicher Ansatz, die friedliche Nutzung des Cyberraums zu fördern.

Dual-use und die Dilemmata für Cybersicherheit, Frieden und Technikbewertung stehen im Mittelpunkt des folgenden Beitrags. Viele Techniken, die hohen Nutzen stiften, können gleichzeitig zur Verursachung erheblicher Schäden genutzt werden (Dual-use-Dilemma). Dem versucht man mit einem Spektrum von Maßnahmen – von Transparenz bis zu gesetzlichen Regelungen – zu begegnen. Weitere Maßnahmen sind Technologiebewertung und Zivilklauseln an Hochschulen, die militärische Forschung einschränken oder verbieten.

Der letzte Beitrag dieses Abschnitts befasst sich mit Maßnahmen des Aufbaus von Vertrauen und Sicherheit. Die Vorbereitung offensiver Akte der Cyberkriegführung führt zu militärischer Instabilität und muss daher eingedämmt werden. Dazu können vertrauensbildende Maßnahmen beitragen. Entsprechende Initiativen gibt es im akademischen, im staatlichen und im internationalen Bereich.

Ein wesentlicher Ansatz zur Konfliktvermeidung ist *Cyber Arms Control*. Im ersten Beitrag dieses Abschnitts wird die Rüstungskontrolle aus ihrem historischen Kontext heraus entwickelt, und es werden unterschiedliche Ansätze und schrittweise Fortschritte von Rüstungskontrollabkommen und die unterschiedlichen Vorschläge von staatlichen Organisationen, privaten Unternehmen und nichtstaatlichen Organisationen erläutert.

Eine besondere Herausforderung für die Rüstungskontrolle stellen unbemannte Systeme dar. Gleichzeitig nimmt ihre Bedeutung für militärische Operationen zu. Kritisiert werden autonome Systeme aus technischer, ethischer und rechtlicher Sicht. Sie können die internationale Sicherheit destabilisieren und müssen entsprechend kontrolliert werden. Die Folgen, die sich ohnehin aus der Nutzung von Software, Automation, Autono-

mie und Künstlicher Intelligenz ergeben, sind im militärischen Bereich noch gravierender als im zivilen Bereich – auch wenn die Probleme grundsätzlich die gleichen sind.

Die Verifikation von Maßnahmen der Rüstungskontrolle wird im letzten Beitrag dieses Abschnitts beschrieben. Im Cyberspace gibt es spezielle technische Rahmenbedingungen, die die Verifikation erschweren. Etablierte Maßnahmen werden auf ihre Probleme bei der Anwendung im Cyberspace untersucht. Danach werden Ansätze zur Verifikation im Cyberspace erläutert.

Ein Problem der Cyberkriegführung ist die Attribuierung, also die Zuordnung von Angriffen zu einem Angreifer. Die Möglichkeiten und Schwierigkeiten bei der Attribuierung von Angriff en behandelt der erste Beitrag des Abschnitts *Cyber Attribution and Infrastructures*. Nach der Erläuterung der grundlegenden Prinzipien folgen die speziellen Probleme bei *Malware* und *Advanced Persistent Threats* und bei der Attribuierung im Cyberkrieg. Attribuierung ist weiterhin ein komplexes und ungelöstes Problem.

Resiliente kritische Infrastrukturen sind für die Abwehr von Angriffen von besonderer Bedeutung. Deswegen müssen kritische Infrastrukturen resilient konstruiert werden. Die Bedeutung der Resilienz bei kritischen Infrastrukturen, ihre Definition und Modelle zu ihrer Konstruktion sind Thema des nächsten Beitrags. Dabei wird auch zwischen den englischen Begriffen *safety* und *security* differenziert: Während *safety* sich vor allem auf die Zuverlässigkeit und Fehlertoleranz der Systeme bezieht, die auf der langfristigen Nutzung sicherer Konfigurationen fußen, meint *security* die Fähigkeit, sich laufend ändernde Bedrohungen abzuwehren und dafür stetig angepasst zu werden – ein Zielkonflikt, der aufgelöst werden muss.

Von besonderer Bedeutung ist die Sicherheit (*security*) kritischer Informations-Infrastrukturen. Der letzte Beitrag des Abschnitts untersucht deren Grundsätze, ihre Schlüsselcharakteristika und Funktionalität und die Risiken und Bedrohungen, denen sie ausgesetzt sind. Ein Phasenmodell des Schutzes kritischer Infrastrukturen wird vorgestellt, das von der Analyse über die Umsetzung von Schutzmaßnahmen, Überwachung, Behandlung von Störungen, Wiederherstellung und Verbesserung, Schulung und Wissensverbreitung bis zur Bestätigung und Zertifizierung reicht.

Im Abschnitt *Culture and Interaction* werden zu Beginn erneut die Konzepte von Sicherheit im Sinne von *safety* und *security* vorgestellt, ergänzt um deren zugrundeliegende Theorien und Methodologien. Die Entstehung und Bedeutung von Sicherheitskulturen wird erläutert und das sich ändernde Verhältnis von technologischen zu politischen Problemen reflektiert.

Die beiden weiteren Beiträge des Abschnitts lenken den Blick auf die sozialen Medien. Zunächst stehen kulturelle Aspekte im Fokus: das Verhältnis sozialer Medien und der ihnen zugrundeliegenden Informations- und Kommunikationstechnologien zu Gewalt und Frieden. Kulturelle Eingriffe durch Nutzer sozialer Medien wie auch durch Social Bots können Konflikte anheizen, aber auch gesellschaftlichen Frieden fördern. Die interessengeleitete Nutzung von sozialen Medien und von Informations- und Kommunikationstechnologien durch unterschiedliche Akteure in Konflikten wird im letzten Beitrag dieses Abschnitts angesprochen und kritisch betrachtet.

Den Abschluss des Bandes bildet ein *Outlook*, der von den AutorInnen des Lehrbuchs gemeinsam zusammengestellt wurde. Hier werden aktuelle Trends und abzusehende künftige Entwicklungen vorgestellt und bewertet. Die AutorInnen gehen davon aus, dass die Unsicherheit durch informationstechnische Angriffe und damit der Bedarf an technischen Lösungen und internationalen Abkommen zur Reduzierung des Risikos weiter zunehmen werden.

Von einem Lehrbuch erwartet man, dass es die wesentlichen Aspekte seines Themengebiets umfassend und auf Basis aktueller wissenschaftlicher Erkenntnisse behandelt. Diesem Anspruch wird der Band gerecht. Zahlreiche Beispiele realer Cybervorfälle illustrieren den Inhalt. Die Bedeutung der Informationstechnologie für Frieden, Sicherheit und Konflikte wird weiter zunehmen, wie regelmäßig Berichte in den Medien zeigen. Dies zeigt der Band auf, indem er aktuelle Trends und Entwicklungen im Ausblick zusammenstellt. Er bietet damit entsprechend seiner Zielsetzung eine gute und umfassende Einführung in die Thematik.

Der Zusammensetzung des Bandes aus Beiträgen einzelner Autorinnen und Autoren ist wohl geschuldet, dass die Themen nicht immer klar abgegrenzt sind. So erläutert das Kapitel zur Spionage beispielsweise viele Grundlagen der IT-Sicherheit, die auch für andere Bereiche relevant sind und deswegen in einen eigenen Grundlagenabschnitt ausgelagert werden sollten. Im Beitrag über das Darknet werden ausführlich die Grundlagen von Konflikten referiert und die mit dem *Framing* verbundenen Probleme erläutert. Die eigentliche Thematik, das Darknet, kommt im Vergleich dazu zu kurz. Mit vielen Querverweisen wird versucht, inhaltliche Verknüpfungen herzustellen. Dennoch würde eine stringentere, übergreifende Strukturierung den Wert des Bandes noch erhöhen.

Für eine zweite Auflage würde ich mir eine intensivere Behandlung von Verfahren der Spieltheorie, der Künstlichen Intelligenz und des Maschinellen Lernens im militärischen Bereich wünschen – die Nutzung sowie Möglichkeiten und Grenzen sowohl für Cyberoperationen und IT-Sicherheit als auch für Verifikation und Forensik. Auch die Konsequenzen daraus – die Frage der Realisierbarkeit, Möglichkeiten und Probleme einer Maschinenethik – könnten ausführlicher behandelt werden. Ein Abschnitt zu Ansätzen des Transhumanismus imMilitär wäre ebenfalls wünschenswert. Dazu könnten die Verflechtungen von Wissenschaft und Forschung – insbesondere an Hochschulen – Inhalt eines weiteren Abschnitts sein.

In Summe tun diese Kritikpunkte dem Wert des Bandes aber keinen Abbruch. Wer sich einen fundierten Überblick über die aktuellen Entwicklungen der Informationstechnologie für Frieden und Sicherheit verschaffen will, dem ist dieses Buch zu empfehlen.

Die Rezension erschien zunächst in Wissenschaft & Frieden 4/2019. Wir danken der Redaktion für die freundliche Genehmigung zum Nachdruck.

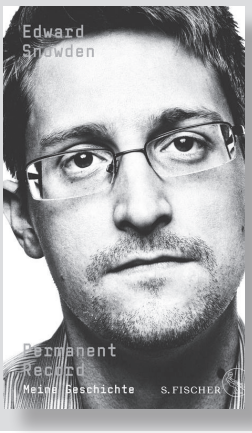
Dietrich Meyer-Ebrecht

Edward Snowden: Permanent Record – Meine Geschichte

Sie wollen alles wissen, sie wollen alles sammeln, für alle Zeiten – the *Permanent Record*: Es bedurfte einiger Jahre in unterschiedlichen Abteilungen und Auslands-Dependancen der NSA und der CIA, bis Snowden bewusst wird, dass die US-Geheimdienste im Begriff sind, ein Überwachungsnetz unvorstellbaren Ausmaßes aufzubauen. Zunächst ist es eine vage Ahnung. Aber die treibt ihn an, sich Gewissheit zu verschaffen, Spuren nachzugehen, nach internen Dokumenten zu recherchieren, selber zum Sammler zu werden. Und schließlich fordert sein Gewissen, der Öffentlichkeit die Ungeheuerlichkeit des Tuns und der Pläne der Geheimdienste zu enthüllen, mit den gesammelten Dokumenten als Beweismaterial. *Permanent Record – Meine Geschichte* ist Snowdens sehr persönliche Erzählung. Er beginnt mit Erinnerungen aus seiner Jugendzeit, schreibt über Menschen, Erlebnisse und Ereignisse, die ihn geprägt haben, und lässt uns seinen Weg zum Wistleblower miterleben – Stoff für einen Agententhriller …

Der 11. September 2001 verändert alles. Ein patriotischer Weckruf geht durch alle Schichten der US-amerikanischen Gesellschaft. Snowden, gerade 18 Jahre alt und aus einem patriotischen Elternhaus stammend, sieht es als seine staatsbürgerliche Pflicht, in dieser Stunde seinem Volk zu dienen, und wie viele andere junge Menschen meldet er sich 2004 zum Militär. In seiner Enttäuschung nach dem baldigen Abbruch seiner Ausbildung wegen einer ernsthaften Verletzung sucht er nach einer Möglichkeit, seine Fertigkeiten an anderer Stelle für sein Volk einzubringen: Die NSA, die wie alle anderen US-Geheimdienste in dem nun herrschenden politischen Klima ihre Kompetenzen und Mittel enorm ausbauen kann, sucht IT-Experten, zu jener Zeit eine rare Spezies. Und Snowden ist einer dieser jungen Exoten.

Snowden wird 1983 geboren, in dem Jahr, in dem das TCP/IP als universelles Kommunikationsprotokoll für alle im Internet vermittelten Daten eingeführt wird. Es wird der weltweiten Vernetzung einen entscheidenden Anschub geben. Noch im Grundschulalter darf Snowden einfache Programmbefehle auf dem Commodore 64 seines Vaters tippen. Als er neun ist, kauft der Vater sich seinen ersten PC, einen Compaq Pesario. „Der Compaq wurde mein ständiger Begleiter", erinnert er sich, „mein zweites Geschwister, meine erste Liebe." Für mich als Leser war es ein Déjà-vu, wenn er beschreibt, wie er sich über ein 14,4-kBaud-Modem in Rechenzentren einwählt – ich habe die kryptische Melodie der Synchronisation über die analoge Telefonleitung noch im Ohr … Er klinkt sich in die *bulletin boards* ein, landet mit *Telnet* auf der Konsole zentraler Rechenanlagen – auch schon einmal unautorisiert. Er entdeckt im Web 1.0 eine neue, ungeahnte Welt, eine Welt der Freiheit, der Offenheit, der unbegrenzten Möglichkeiten. „Ich war eines der *script kiddies*", schreibt er, die ihre Kenntnisse schnipselweise aus *bulletin boards* und Diskussionsforen zusammentrugen und untereinander auf hektographierten Zetteln verbreiteten. So eignet er sich ein sehr fundamentales Wissen über die Mechanismen der Informationstechnik an. Teils eher zufällig, teils mit gezielten Experimenten, dringt er auch schon einmal in in die abgeschlossen Datenreiche staatlicher Institutionen ein, aus reiner Neugier. Wer denkt damals schon an die mannigfaltigen Missbrauchsmöglichkeiten, die sich mit dem Ausbreiten des Netzes und seinem Eindringen in alle Lebensbereiche anbieten sollten? Die von den Möglichkeiten faszinierten glauben naiv, dass die *community* nur aus neugierigen, wissbegierigen, experimentierfreudigen *freaks* besteht.



Edward Snowden (2019)
Permanent Record
Verlag: S. Fischer
428 Seiten
Preis 22,00 €
ISBN: 978-3-10-397482-9

Snowden gehört zu der Generation, deren Kenntnisse und Erfahrungen mitwachsen mit den rasch komplexer und raffinierter werdenden Hardware-, Software- und Netzwerktechnologien. Diese Generation erlebt mit, wie das ursprünglich dezentral konzipierte Internet, eine anarchische, basisdemokratische Domäne, zunehmend von staatlichen Institutionen und gewinnorientierten Unternehmen in Beschlag genommen wurde und sich zu einer Netzwelt mit immer stärker zentralisierten Zügen entwickelt. Diesen Prozess aktiv mitzuerleben, gibt dieser Generation die nicht wiederholbare Chance, ein Wissen aufzubauen, das noch in den entwicklungsgeschichtlichen Ursprüngen wurzelt, und darauf aufbauend ein ganzheitliches Verständnis zu entwickeln. Zu einer Zeit, als es noch Generalisten geben konnte, rekrutieren sich aus dieser Generation *computer professionals*, die die Informationstechnik von ihrer grundlegenden Substanz her begreifen, die ein intuitives Verhältnis zu ihr haben. Und die sucht die NSA zur Umsetzung ihrer Vorstellungen von einer weltweiten Überwachung für die Abwehr terroristischer Aktivitäten – händeringend.

2009 bewirbt sich Snowden bei der NSA und wird sofort eingestellt, auch ohne den eigentlich obligatorischen akademischen Abschluss. Zwar steht er auf der Gehaltsliste des IT-Dienstleisters Dell und bleibt es auch während der gesamten Tätigkeit für die NSA (ausgenommen zuletzt für drei Monate bei Booz Allen Hamilton). De facto ist sein Status jedoch der eines genuinen Mitarbeiters der NSA – auch wenn das später offiziell anders dargestellt wird, um seinen Mitarbeiterstatus herabzuspielen. Snowden wird dank seines Wissens und seiner Erfahrungen sehr bald mit komplexen Aufgaben betraut. Er wird ins Ausland delegiert, arbeitet in der US-Botschaft in Genf, später in Tokio, arbeitet zeitweise *undercover* für die CIA. Er lernt die IT-Instrumente und -Infrastruktur der Geheimdienste detailliert kennen – und da er im Gegensatz zu vielen seiner eng auf ihre IT-Tätigkeit fokussierten Mitarbeiter neugierig und aufgeschlossen für seine Umgebung ist, eröffnen sich ihm interessante Einblicke in die

Arbeitsweise der Geheimdienste, zumal er dank seiner Zugriffsrechte als Systemadministrator selbst zu hochvertraulich eingestuftem Material Zugang hat. Seine Zugriffsrechte werden noch einmal umfassender, als er mit Arbeiten zur Zusammenführung der heterogenen Systeme von CIA und NSA betraut wird. Nicht einmal leitende Mitarbeiter in höchsten Positionen, stellt er fest, verfügen über derart umfassende Zugriffsrechte wie die mit übergreifenden Administrationsarbeiten betrauten Mitarbeiter.

In Tokio springt er für einen Mitarbeiter ein und übernimmt dessen Aufgaben im Rahmen einer Schulungsveranstaltung über die IT-gestützten Ausspähtechniken des chinesischen Geheimdienstes. Erst die Recherche in den von der NSA zusammen getragenen Dokumenten zu diesem Thema – hier kommen ihm seine umfassenden Zugriffsrechte zur Hilfe – öffnen ihm die Augen für die grenzenlosen Möglichkeiten, eine ganze Gesellschaft bis zu ihrem letzten Individuum, bis in den letzten privaten Winkel auszuspähen – und welche ungeahnte Machtfülle der Staat damit über seine BürgerInnen gewinnen kann. Ein Verdacht keimt in ihm: Was China kann, was der chinesische Geheimdienst mit seinen Bürgern macht, macht es womöglich die NSA im Geheimen bereits mit der ganzen Welt? Arbeitet auch die NSA bereits an einem Überwachungsprogramm globalen Ausmaßes, an einem Programm, das auch die eigenen BürgerInnen erfasst, das die in der Verfassung der Vereinigten Staaten verbrieften Freiheitsrechte unterminiert, das an Legislative, an Exekutive und an allen politischen Instanzen vorbei getrieben wird?

Die Vorstellung einer alles erfassenden Überwachung ist weder mit seiner ethischen Überzeugung noch mit seiner patriotischen Einstellung vereinbar. Snowden will Beweise. Von nun an durchsucht er das Intranet der NSA systematisch nach Dokumenten, die ihm Einblick in die Programme der NSA geben. Anfänglich ist er nur auf der Suche nach einer Bestätigung für seinen Verdacht, dass ein amerikanisches Massenüberwachungssystem bereits existiert. Aber dann will er auch wissen, wie dieses System funktioniert. Er trägt zusammen, was er finden kann, zunächst ohne bewussten Plan, was er damit machen wird. Den zeitlichen Freiraum während seiner Dienststunden verschafft er sich, indem er jede neue Routineaufgabe, die er im Rahmen seiner Administrationstätigkeit übernimmt, sogleich automatisiert. Seine jetzige und letzte Dienststelle in Kunia auf der Hawaii-Insel Oahu bietet ihm als dem einzigen Mitarbeiter des *Office of Information Sharing* gute Möglichkeiten, seine Recherchen zu verschleiern und seine *Sammlung* zu verbergen.

Dass das Überwachungsprogramm der NSA in eklatanter Weise die Verfassung der USA verletzt, gibt Snowden den entscheidenden Impuls, zum Whistleblower zu werden. Seine Entscheidung ist gleichzeitig ein Schritt in die Einsamkeit und Isolation. Kollegen, mit denen er andeutungsweise darüber spricht, zucken nur die Schultern. Lindsay, seiner langjährigen Partnerin, muss er seinen Plan verschweigen, um sie nicht als Mitwisserin in Gefahr zu bringen. Die letzten Monate auf Hawaii ist er damit beschäftigt, seinen Riesenfundus an internen und vertraulichen Dokumenten unentdeckt aus seiner Dienststelle herauszuschaffen und unter großen Vorsichtsmaßnahmen auf die schwierige Suche nach Journalisten zu gehen, von denen er eine zuverlässige Unterstützung für seine Enthüllungen erwarten kann. Mit Laura Poitras und Glenn Greenwald wird ein Treffen in Hongkong vereinbart.

Mitte Mai 2013 schnürt Snowden leichtes Gepäck und fliegt, mit bar bezahlten Tickets, über Tokio nach Hongkong. Poitras' und Greenwalds Ankunft verzögert sich, für Snowden eine nervenzehrende Wartezeit in der panischen Angst, dass sein Vorhaben scheitern könnte und er alle Risiken vergeblich eingegangen wäre. Am 2. Juni erscheinen sie endlich. Die ersten Enthüllungen schlagen weltweit ein. Dann folgen drei weitere Wochen zermürbenden Wartens, bis der Weg gebahnt ist in ein Land, das keinen Auslieferungsvertrag mit den USA hat, Ecuador. Sarah Harrison, Journalistin und Mitarbeiterin von Wikileaks, ist gekommen, um Snowden zu unterstützen. Sie begleitet ihn auf dem Flug mit dem Ziel Quito, via Moskau und Havanna, um den Luftraum von militärisch mit den USA kooperierenden Staaten so gut wie möglich zu umgehen. Am 23. Juni findet der Flug sein ungeplantes Ende bereits in Moskau. Snowden darf nicht wieder aus Russland ausreisen, denn die US-Behörden haben seinen Pass annulliert. Seitdem lebt Snowden, nun bereits im siebten Jahr, in Moskau im Exil, seit drei Jahren mit Lindsay, die ihm gefolgt ist – vor zwei Jahren haben sie geheiratet.

Permanent Record – Meine Geschichte ist ein ein lesenswertes und ein sehr wichtiges Buch, hochinteressant nicht zuletzt auf Grund der Fülle an Hintergrundinformationen. So nimmt uns Snowden auf seinem Weg durch seine verschiedenen Arbeitsorte mit in die Welt der *intelligence community*, der Nachrichten- und Aufklärungsdienste, und vermittelt uns en passant aufschlussreiche Einblicke in deren Denken und Wirken. Das Buch liest sich flüssig, und am Ende wird es richtig spannend. Man merkt dem Text die professionelle Unterstützung an – Snowden würdigt sie im Nachspann, die wertvolle Hilfe vieler Köpfe bei der Strukturierung des Stoffes und der Niederschrift der vielen Details. Auch dem Übersetzer gelingt es gut, diese Authentizität wiederzugeben.

Das Buch erscheint zu einer Zeit, in der wir bereits aus den Augen verloren haben, welche Ungeheuerlichkeiten Snowden enthüllt hat. So bleibt nach dem Lesen des Buches ein ungutes Gefühl: Was wurde aus dem riesigen Fundus an Material gemacht, das Snowden unter höchsten persönlichen Risiken und mit der Konsequenz einer nachhaltigen persönlichen Einschränkung beschafft hat? Die Veröffentlichung einer Reihe spektakulärer Details hat die öffentliche Empörung entflammt, für eine kurze Zeit. Und schon ist das öffentliche Interesse – und damit das Engagement der Medien – wie bei allen Skandalen wieder eingeschlafen. Wenn er es auch nicht durchblicken lässt, für Snowden muss das eine herbe Enttäuschung sein. Denn er hat nicht die punktuellen Übergriffe – wie etwas den Einbruch in Merkels gesichertes Telefon – publik machen wollen. Er wollte das System aufdecken, die Intention dahinter und das Potenzial, das die NSA bereit hält für eine weltumspannende Überwachung. Snowden wollte mit seinem Material Glaubwürdigkeit erreichen. In diesem Sinne haben die Medien sein Material missbraucht, um daraus eine Reihe von Sensationsstories zu machen. Und dann das Interesse verloren. Sie haben die Chance verpasst, auf der Grundlage diesen Materials offensive Aufklärungsarbeit zu leisten, die Gesellschaft zu sensibilisieren für die Gefahr, im Sog der Technologie in einen Überwachungsstaat à la China hineinzugleiten.

Snowden entlässt uns mit einem Appell an unsere Verantwortung gegenüber unseren Kindern und Enkeln: „Wenn wir den

Anspruch an unsere Daten jetzt nicht zurückfordern, wird es für unsere Kinder vielleicht zu spät sein. […] Jede zukünftige Generation wird […] der ungeheuerlichen Anhäufung von Information unterworfen sein […], deren Potential zur Kontrolle der Gesellschaft und Manipulation jedes Einzelnen nicht nur die gesetzlichen Beschränkungen sprengt, sondern auch jegliche Vorstellungskraft."

Wissenschaft & Frieden 4/2019 „Ästhetik im Konflikt"

Bei der Verleihung des Friedenspreises des deutschen Buchhandels 2019 an den brasilianischen Photographen Sebastião Salgado leitete Wim Wenders seine Laudatio mit zwei Fragen ein: „Kann Photographieren ein Akt des Friedens sein? Kann die Photographie friedensfördernd sein?" Photographien und andere künstlerische Werke provozieren überdies die Frage, wie die Darstellung von Leid und Zerstörung auf die BetrachterInnen wirkt – verharmlosend, abstoßend, aufklärend, versöhnend, aktivierend? Mit diesen und anderen Fragen befassen sich die Artikel in W&F 4/2019, „Ästhetik im Konflikt".

Es schreiben:

- *Christine Andrä* und *Berit Bliesemann de Guevara*: Konflikttextilien – Analytischer, ästhetischer und politischer Stoff für Friedensforschung und -arbeit
- *Claudia Maya* und *Stefan Peters:* Der zerbrochene Spiegel des Krieges – Der kolumbianische Bürgerkrieg im Werk von Jesús Abad Colorado
- *Christina Hartmann:* Freiheit, Frieden, Gerechtigkeit – Kunst und Kultur in der sudanesischen Revolution
- *Aicha Kheinette:* Die Schönheit der Bombe – Zur Ästhetik im nuklearen Diskurs
- *Tim Bausch:* „House Demolitions" – Eine szenische Darstellung ästhetischen Widerstandes
- *Michaela Zöhrer:* Schreckensbilder für den Frieden? Zur Rolle gewaltvoller Bilder in Geschichte und Gegenwart
- *Anne Maximiliane Jäger-Gogoll:* „Verblendung" als Aufklärung – Eine Gedenkinstallation für die Opfer der „Marburger Jäger"
- *Michael Jenewein:* Menschwerdung im Krieg – Bundeswehr in den Fußstapfen von Ernst Jünger?
- *Dieter Senghaas:* Komponierbare Friedensproblematik?

Außerhalb des Schwerpunktes denken *Christine Schweitzer* und *Helmut Lohrer* darüber nach, ob Sanktionen ein geeignetes friedenspolitisches Instrument sind, *Senta Pineau* blättert die zehnjährige Geschichte der Zivilklausel in Nordrhein-Westfalen auf und *Karlheinz Lipp* stellt anlässlich dessen 50. Todestages den Friedensaktivist und -arbeiter Friedrich Siegmund-Schultze vor.

Der Gastkommentar von *Jochen Hippler* wirft einen Blick auf den aktuellen Konflikt in Kaschmir und die kommentierte Presseschau beleuchtet die Reaktionen auf den Einmarsch der Türkei in Nordsyrien.

Wissenschaft & Frieden, 4/2019: „Ästhetik im Konflikt". 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: *vertrieb@wissenschaft-und-frieden.de*, *www.wissenschaft-und-frieden.de*

Wissenschaft und Frieden ist Trägerin des Göttinger Friedenspreises 2018

FIfF e.V.

Im FIfF haben sich rund 700 engagierte Frauen und Männer aus Lehre, Forschung, Entwicklung und Anwendung der Informatik und Informationstechnik zusammengeschlossen, die sich nicht nur für die technischen Aspekte, sondern auch für die gesellschaftlichen Auswirkungen und Bezüge des Fachgebietes verantwortlich fühlen. Wir wollen, dass Informationstechnik im Dienst einer lebenswerten Welt steht. Das FIfF bietet ein Forum für eine kritische und lebendige Auseinandersetzung – offen für alle, die daran mitarbeiten wollen oder auch einfach nur informiert bleiben wollen.

Vierteljährlich erhalten Mitglieder die Fachzeitschrift FIfF-Kommunikation mit Artikeln zu aktuellen Themen, problematischen Entwicklungen und innovativen Konzepten für eine verträgliche Informationstechnik. In vielen Städten gibt es regionale AnsprechpartnerInnen oder Regionalgruppen, die dezentral Themen bearbeiten und Veranstaltungen durchführen. Jährlich findet an wechselndem Ort eine Fachtagung statt, zu der TeilnehmerInnen und ReferentInnen aus dem ganzen Bundesgebiet und darüber hinaus anreisen. Darüber hinaus beteiligt sich das FIfF regelmäßig an weiteren Veranstaltungen, Publikationen, vermittelt bei Presse- oder Vortragsanfragen ExpertInnen, führt Studien durch und gibt Stellungnahmen ab etc. Das FIfF kooperiert mit zahlreichen Initiativen und Organisationen im In- und Ausland.

FIfF-Mailinglisten

FIfF-Mailingliste
An- und Abmeldungen an:
http://lists.fiff.de/mailman/listinfo/fiff-L
Beiträge an: *fiff-L@lists.fiff.de*

FIfF-Mitgliederliste
An- und Abmeldungen an:
http://lists.fiff.de/mailman/listinfo/mitglieder

Mailingliste Videoüberwachung:
An- und Abmeldungen an:
http://lists.fiff.de/mailman/listinfo/cctv-L
Beiträge an: *cctv-L@lists.fiff.de*

FIfF online

Das ganze FIfF
www.fiff.de
Twitter FIfF e.V. – *@FIfF_de*

Cyberpeace
cyberpeace.fiff.de
Twitter Cyberpeace – *@FIfF_AK_RUIN*

Faire Computer
blog.faire-computer.de
Twitter Faire Computer – *@FaireComputer*

Mitglieder-Wiki
https://wiki.fiff.de

FIfF-Beirat

Ute Bernhardt (Berlin); **Peter Bittner** (Kaiserslautern); **Dagmar Boedicker** (München); Dr. **Phillip W. Brunst** (Köln); Prof. Dr. **Wolfgang Coy** (Berlin); Prof. Dr. **Wolfgang Däubler** (Bremen); Prof. Dr. **Christiane Floyd** (Hamburg); Prof. Dr. **Klaus Fuchs-Kittowski** (Berlin); Prof. Dr. **Michael Grütz** (Konstanz); Prof. Dr. **Thomas Herrmann** (Bochum); Prof. Dr. **Wolfgang Hesse** (Marburg); Prof. Dr. **Wolfgang Hofkirchner** (Wien); Prof. Dr. **Eva Hornecker** (Weimar); **Werner Hülsmann** (Konstanz); **Ulrich Klotz** (Frankfurt); Prof. Dr. **Klaus Köhler** (Mannheim); Prof. Dr. **Jochen Koubek** (Bayreuth); Prof. Dr. **Herbert Kubicek** (Bremen); Dr. **Constanze Kurz** (Berlin); Prof. Dr**. Klaus-Peter Löhr** (Berlin); **Werner Mühlmann** (Oppung); Prof. Dr. **Frieder Nake** (Bremen); Prof. Dr. **Rolf Oberliesen** (Bremen); Prof. Dr. **Arno Rolf** (Hamburg); Prof. Dr. **Alexander Rossnagel** (Kassel); **Ingo Ruhmann** (Berlin); Prof. Dr. **Gerhard Sagerer** (Bielefeld); Prof. Dr. **Gabriele Schade** (Erfurt); **Ralf E. Streibl** (Bremen); Prof. Dr. **Marie-Theres Tinnefeld** (München); Dr. **Gerhard Wohland** (Waldorfhäslach)

FIfF-Vorstand

Stefan Hügel (Vorsitzender) – Frankfurt am Main
Rainer Rehak (stellv. Vorsitzender) – Berlin
Michael Ahlmann – Kiel / Blumenthal
Maximilian Hagner – Jena
Alexander Heim – Berlin
Sylvia Johnigk – München
Prof. Dr. **Hans-Jörg Kreowski** – Bremen
Kai Nothdurft – München
Jens Rinne – Mannheim
Prof. Dr. **Britta Schinzel** – Freiburg im Breisgau
Ingrid Schlagheck – Bremen
Anne Schnerrer – Berlin
Prof. Dr. **Werner Winzerling** – Fulda

FIfF-Geschäftsstelle

Ingrid Schlagheck (Geschäftsführung) – Bremen
Philipp Love – Bremen

Impressum

Herausgeber	Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e. V. (FIfF)
Verlagsadresse	FIfF-Geschäftsstelle Goetheplatz 4 D-28203 Bremen Tel. (0421) 33 65 92 55 *fiff@fiff.de*
Erscheinungsweise	vierteljährlich
Erscheinungsort	Bremen
ISSN	0938-3476
Auflage	1 200 Stück
Heftpreis	7 Euro. Der Bezugspreis für die FIfF-Kommunikation ist für FIfF-Mitglieder im Mitgliedsbeitrag enthalten. Nichtmitglieder können die FIfF-Kommunikation für 28 Euro pro Jahr (inkl. Versand) abonnieren.
Hauptredaktion	Dagmar Boedicker, Stefan Hügel (Koordination), Sylvia Johnigk, Hans-Jörg Kreowski, Dietrich Meyer-Ebrecht, Ingrid Schlagheck
Schwerpunktredaktion	Dagmar Boedicker
V.i.S.d.P.	Stefan Hügel
Retrospektive	Beiträge für diese Rubrik bitte per E-Mail an *redaktion@fiff.de*
Lesen, SchlussFIfF	Beiträge für diese Rubriken bitte per E-Mail an *redaktion@fiff.de*
Layout	Berthold Schroeder, München
Cover	Salomé von Sebastian Hertrich, Foto: Anna Franke. Siehe dazu auch Seite 6.
Druck	Meiners Druck, Bremen Heftinhalt auf 100 % Altpapier gedruckt.

KLIMAneutral produziert

Die FIfF-Kommunikation ist die Zeitschrift des „Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e. V." (FIfF). Die Beiträge sollen die Diskussionen unter Fachleuten anregen und die interessierte Öffentlichkeit informieren. Namentlich gekennzeichnete Artikel geben die jeweilige Autor.innen-Meinung wieder.

Die FIfF-Kommunikation ist das Organ des FIfF und den politischen Zielen und Werten des FIfF verpflichtet. Die Redaktion behält sich vor, in Ausnahmefällen Beiträge abzulehnen.

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*)

FIfF-Klausur
3.-5. April, Jugendherberge, Fulda

FIfF-Kommunikation

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

2/2020 „Elektronische Gesundheitskarte"
Werner Winzerling u. a.
Redaktionsschluss: 1. Mai 2020

Zuletzt erschienen:
1/2019 Brave new World 1
2/2019 Brave new World 2
3/2019 Cyberpeace und IT-Security

W&F – Wissenschaft & Frieden
1/19 70 Jahre NATO
2/19 Partizipation – Basis für den Frieden
(mit Dossier 89: Verifikation nuklearer Abrüstung)
3/19 Hybrider Krieg?
4/19 Ästhetik im Konflikt

vorgänge – Zeitschrift für Bürgerrechte und Gesellschaftspolitik
#225/226 Wandel der Kommunikationsfreiheit durch Digitalisierung und Internet
#227 Polizei und Technikeinsatz
#228 Wohnen als soziales Grundrecht

DANA – Datenschutz-Nachrichten
1/19 Social Media
2/19 Ein Jahr DSGVO – ein Résumé
3/19 Real Time Bidding
4/19 Datenschutz in Zeiten des Brexit

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

Mietmarkt

Wohnungsgesuche

Berufstätiges Paar sucht Wohnung Er (30, Neurologe, Klinikum Großstadt) sie (25, Gesundheitsmanagerin) suchen Wohnung im Südwesten. 2-3 Zimmer, 50-75 m². ☎ **0177123456**

Archtektin und Informatiker suchen Altbau-Wohnung zur Miete, mind. 65 m², mind. 2,5 Zi., Balkon/Terrasse, Parkett. Ab 1.1. oder später. ☎ **0177123456.**
Email: whng@mailbox.de

Gut situierter Beamter und festang. Akademikerin mit Kind suchen ab 1.1.2020 eine 4-5 ZKB-Wohnung o. Haus im Nordwesten und Umgebung Balkon od. Garten, Stellpl. od. G langfr. Mietverhältnis erwünscht, K bis 1.800 €. **ab@next.org | 01793**

Ist Ihre Wohnung zu groß
Tauschen Sie mit uns! Nette Fami bietet 3 Zi., 80 m2, heller Altbau, I nenstadt, 1. OG, Miete vsl. 800€. N im Tausch gegen 4-5 Zi. zentrum nah, max. 1.800 € kalt ☎ 017712345 **tauschwohnung1@gmx.de**

2-Zimmer-Wohnung: Beamte (Patentprüfer, 33, Nichtrauche keine Haustiere) sucht 2-Zimmer-Wohnung in zentraler Lage.
Einzugstermin völlig flexibel, bis spätestens 1. April 2020
☎ 0177321456
anton_tirol@gmx.de

WIR: männlich, 22 und 23, berufstätig, Nichtraucher, ledig, SUCHEN 2-3 Zimmerwohnung in der Innenstadt. MAX. 1700,-€ warm, ☎ **0176123456**

Fröhliche, zuverlässige, berufstätige Akademikerin, sucht 1-2 Zi.-Wohnung, unbefr. angestellt, Nichtraucherin, keine Haustiere. 1.2., bis 900€ warm, vorzugsweise im Süden der Stadt, ☎ **0177123456**

Wohnung gesucht Paar sucht 1 Zi.-Wohnung nahe Univiertel max. 850€ ☎**+49177123456**

Familie sucht Wohnung 3 köpfige Familie sucht wegen Eigenbedarf eine Wohnung ab 3 Zi.1800 € & 80 m² mit gutem Anschluss an den Willi-Brandt-Platz. Wir freuen uns über jeden Hinweis ☎ **0178456123**

Augsburgerin sucht Wohnung Ich suche für meine kleine Familie (zwei Erwachsene, ein Baby) eine Wohnung mit mindestens 3 Zimmern in München, möglichst zentral gelegen, ein Balkon wäre schön, bis ca. 1600 € warm, ab März/April. Ich bin wissenschaftliche Mitarbeiterin an der Uni, [illegible] ☎ [illegible]

Junge WG (5 sicherheitsbewusste Informatiker*innen mit 2 Kindern + 2 Katzen) sucht REH/alleinstehendes Haus mit großem Garten, überwachungsfrei nach Freiheitsbestands-Analyse. Wir sind friedensbewegt und umweltbewusst.
E-Mail: jungeWG@fiff.de
☎ **0177123456**

Dringend! 28 jähriger Erzieher sucht möglichst zentrale 1-2 Zimmer Wohnung in München. Unbefristet, frühestens 1.12.19, max. €800,- warm
☎ +49172422123

1-Zimmer-Wohnung Doktorand, Allgemeine und Vergleichende Literaturwissenschaft an der LMU, sucht 1-Zimmer-Wohnung mit und ohne Möbel ☎ **01756633987**

Prom. Ärztin (Handchirurgie) s. f. Tochter (Jurastudentin, bald Rechtsreferend., NR, langfr. 1-2 ZKB, Nh. LMU (Mü. Maxvorst., Schwabing, Lehel, Glockenbach Haidhs.) bis max. 850,- WM ☎ **0176/422123**

Medizinstud. sucht
Wir (Arzt u. Soz.päd) su. dringend f. Tochter, 21J Medizinstud., ab Mrz. ein WG-Zi. o. 1-Zi.Ap. o. 2.-Zi-Wo. i. München
☎ +4917735521456

Für unseren Sohn, seit 40 Jahren hier wohnend, Chefredakteur suchen wir nach dem Tod seiner Lebensgefährtin, Ende des Jahres eine kleinere Wohnung. Angedacht: 3-4 TKBB, bevorzugt in der City.
Wir Eltern stehen für Rückfragen, Sicherheiten, Kautionen usw. zur Verfügung und freuen uns, wenn Sie auf uns zukommen. Wir rufen gerne zurück und kommen auch zu Ihnen, um uns, gemeinsam mit unseren Sohn Ihnen vorzustellen.
Danke! **Tel. 0611/172589 E-mail: Info@irgenwasverlag.de**

Frankfurt sucht München Ärztin aus Frankfurt sucht ab sofort eine kleine Wohnung / Zimmer für ihren Sohn, der ab März in München Informatik stuideren möchte. Alle Unterlagen (Schufa, Einkommensnachweis etc.) liegen direkt [illegible] ☎ **0157444456**

Univ.-Prof. im Ruhestand und Ehefrau sucht für Sohn (19), Jurastudent an der Universität, NR, ab sofort 1 Zimmer-Wohnung oder Zimmer bis € 00 warm.
☎ **0172-6893125**

Zuverlässige & unkomplizierte Mieter Diplom-Physiker & Juristin suchen 3 ZKB zum 1.2./1.3. im Radius von 2 km um den Platz der Republik, Nichtraucher, keine Haustiere. **Zuschriften** ✉ **ZS5555321**

Krankenschwester sucht Wohnung
Ich suche eine Wohnung ab sofort in München. Ich bin von Beruf Gesundheits- und Krankenpflegerin, bin 29 Jahre alt.
☎ **017942123456**

Paar mit Kinderwunsch sucht Zuhause ab 3 Zi, ab 75 m2 mit Terr./Blk bis 1.400,– WM, ruhig, U-/S-Bahn-Strammstr./Tram 10 Min. zu Fuß. Wir: 32 & 36, Akad., unbefr. Arbeitsv., zuverl., umgängl., NR, k. Tiere
☎ **0173-42123456**

Direktor Stadtmuseum
neu in der Stadt sucht ab 2020 zentrale 3-Zi. Whg., 100-140 qm mit Balkon o.ä, & EBK ab 2/2020 für sich und seine Frau zu mieten.
Kontakt mitausblick@gmx.com

Wohnungsangebote

Wohnen am Hirschgarten, 3 Zi., 86 m² Wfl.von privat über bodent. Fenster von 3 Seiten sehr schön belichtet, gr. Bad mit sep. Dusche, Gäste-WC, EBK, TG, ruhig, Blk.
KM €1500 + NK €270 + TG €80, frei ab 01.1.2020
EMail: frei11@gmy.net

Laim/Nähe Westpark 1-Zi., Lift, Blk., Fliesen im Bad ganzwandig, WoZi. Parkett, ca. 37m², €525,- + NK + KT, Bj. 1974, Öl, EA-V, 150,4 kWh/(m²*a) **Fax 089 5589788**

Menterschwaige, traumh. 4-Zi.-Penthouse-DG-Terr.-Whg., ca. 185m² Wfl., 2. OG, hochwert. Ausstatt. u.a. Parkett, EA-V, BJ 70, HZG Öl, EV-W 138 kWh/m²a, €2960,- + NK, nur an seröse Dauermieter. **FRI Immobilien ☎ 5663987**

Lehel/Engl. Garten, App. 20,5 m², 4. OG/Lift, hell, ruh., Küchenzeile, voll renoviert, Blick über München, befristet, EA vorh., WM €675.- v. priv., bei Bedarf Garagenstellpl. in der Nähe
Mail: drilling1@gmy.net

Östl. v. Wasserbirg/Inn, zwei 3-4-Zi.-Whg., 112 und 122 Wohnfl. (KM 10,-/m² + NK), inkl. Balk./Garten zzgl. Gge. u. Stellpl., **Erstvermietung in kl. ländl. Anwesen**, Energiebedarf 33 kWh/m² a/Sonne + Gas.
Optinal - gleicher Energiebedarf, separat neue Gew.-EH, von 40 - 300 m² modulare Aufteilung mögl. (Büro, Kanzlei, ..), von Privat ab Feb. 2020, Näheres unter ☎ **0177/35521456**

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