

E..I..f..F.. Kommunikation

Zeitschrift für Informatik und Gesellschaft

41. Jahrgang 2024

Einzelpreis: 7 EUR

3/2024 – September 2024



Datenschutz überall – außer in der Praxis?

ISSN 0938-3476

• Militarisierung Bildungssektor • Bündnis Opt-out • Klima und KI •

Inhalt

Ausgabe 3/2024

- 03 Editorial
- *Stefan Hügel*

Forum

- 04 Der Brief: ... damit der Traum nicht aus ist.
- *Stefan Hügel*
- 06 #FifKon2024: Nachhaltigkeit in der IT – green coding – open source – green by IT
- *FifF e. V.*
- 07 Einladung zur Mitgliederversammlung 2024
- 07 Cyberpeace – für Frieden, Freiheit und eine lebenswerte Welt
- *Hans-Jörg Kreowski, Aaron Lye, Margita Zallmann*
- 08 Drohender Schaden für die Demokratie
- *Gemeinsamer Appell*
- 10 Biometrischer Überwachungsexzess der Bundesregierung
- *FifF e. V.*
- 11 Widerspruch gegen die elektronische Patientenakte
- *Walter Schmidt*
- 13 Militarisierung des Bildungssektors per Gesetz
- *Rolf Gössner*
- 16 Klima und KI – Vernunft ist nicht alles
- *Sarah Kessler*
- 25 Gegen die unheilvolle Verflechtung von Informatik und Militär
- *hekta und Constanze Kurz im Interview mit Hans-Jörg Kreowski und Rainer Rehak*

Rubriken

- 55 Impressum/Aktuelle Ankündigungen
- 56 SchlussFifF

„Datenschutz überall – außer in der Praxis?“

- 29 Editorial zum Schwerpunkt
- *Jörg Pohle, Stefan Hügel*
- 32 Implementing GDPR: A Perspective from Developers
- *Yuwen Zhang, Frank Ebbers, Nicholas Martin*
- 37 Durchführung einer Datenschutzfolgenabschätzung nach SDM
- *Karin de Lange*
- 43 Warum Checklisten im Datenschutz kaum noch sinnvoll sind. Besser: „einfach.SDM.machen“
- *Thomas Werning*

Netzpolitik.org

- 46 „Kinder haben auch ein Recht auf Privatsphäre“
- *Chris Köver, Charlotte Horsch*
- 48 Der Wert menschlicher Übersetzung
- *Janine Malz*
- 50 Wie Online-Pflicht Menschen ausschließt
- *Martin Schwarzbeck*
- 52 Autoritäre Zeitenwende, schlüsselfertig
- *Anna Biselli*
- 53 Macht endlich wirklich etwas gegen Staatstrojaner
- *Maximilian Henning*

Editorial

Datenschutz überall – außer in der Praxis? So könnte man in Anlehnung an den Nobelpreisträger Robert Solow und Erik Brynjolfsson¹ fragen, wenn man die praktische Umsetzung des Datenschutzes in Organisationen betrachtet. Im Editorial des Schwerpunkts in dieser Ausgabe der FIfF-Kommunikation heißt es dazu:

Seit mehr als fünfzig Jahren gibt es spezielle Datenschutzgesetze, das Bundesdatenschutzgesetz ist 46 Jahre alt, die EG-Datenschutzrichtlinie fast 30 und die EU-Datenschutz-Grundverordnung auch schon wieder sechs Jahre. Die Diskussion um die unerwünschten Eigenschaften und Auswirkungen moderner Informatiksysteme und Informationsverarbeitungen ist sogar noch älter, und selbst die informatische Forschung zu möglichen Gegen- und Schutzmaßnahmen geht der rechtlichen Regulierung zeitlich voraus. Gerade vor diesem Hintergrund überrascht es umso mehr, dass wir ganz offensichtlich noch weit entfernt davon sind, datenschutzfreundliche Systeme in der Breite zu entwickeln und in die Praxis zu bringen.

In drei Beiträgen wird die Frage nach der praktischen Umsetzung des Datenschutzes weiter entfaltet. Das vorangestellte Schwerpunkteditorial führt in die Fragestellung ein, was uns an wirksamem Datenschutz hindert und stellt die einzelnen Beiträge des Schwerpunkts vor.

Es ist eigentlich unnötig, festzustellen, dass das FIfF jede Form von Antisemitismus klar ablehnt. So wäre es grundsätzlich zu begrüßen, wenn der Deutsche Bundestag eine Resolution verabschiedet, die sich ebenso klar vom Antisemitismus distanziert und auch Maßnahmen benennt, wie er wirksam bekämpft werden kann.

Den Resolutionsentwurf, der derzeit die Runde macht², halten wir jedoch gemeinsam mit einer Reihe zivilgesellschaftlicher Organisationen und Einzelpersonen für problematisch:

„Die öffentlich gewordene Fassung der geplanten Resolution des Deutschen Bundestags Nie wieder ist jetzt: Jüdisches Leben in Deutschland schützen, bewahren und stärken, erfüllt uns jedoch mit großer Sorge. Nach ersten juristischen Einschätzungen kollidiert sie mit dem Grundgesetz, bringt eine mannigfaltige Rechtsunsicherheit, zweifelhafte Praktikabilität und die Gefahr der Diskriminierung mit sich“.

heißt es in einem Appell, den wir mitunterzeichnet haben. Er ist in dieser Ausgabe nachzulesen.

Der Anschlag (ausgerechnet) in Solingen³, der drei Todesopfer und mehrere Verletzte gefordert hat, ist furchtbar und zu verurteilen. Leider hat aber auch er wieder zu den sicherheitspolitischen Reflexen geführt, in deren Folge der Abbau von Grundrechten fortgesetzt wird. Die geplante, weitgehende biometrische Überwachung unter Nutzung von Bildern aus dem Internet und Techniken der Künstlichen Intelligenz gefährdet die

Anonymität und hat das Potenzial, uns alle immer und überall identifizierbar zu machen. Wir lehnen mit vielen anderen Organisationen dieses gefährliche Gesetzespaket ab; die Stellungnahme, die wir mitunterzeichnet haben, ist ebenfalls in dieser Ausgabe abgedruckt.

Darauf folgt ein Beitrag zum Widerspruch gegen die elektronische Patientenakte von Walter Schmidt von der Bürgerrechtsvereinigung *Patientenrechte und Datenschutz*. Das FIfF ist ebenfalls Teil eines breiten gesellschaftlichen Bündnisses zur Verteidigung der Selbstbestimmung über die eigenen medizinischen Daten – dies war auch in der Vergangenheit bereits Thema der *FIfF-Kommunikation*.

Die Bestrebungen zur Militarisierung der Gesellschaft schreiten fort – Stichworte *Zeitenwende* und *Kriegstüchtigkeit* –, und Bayern setzt sich wieder einmal in unguter Weise an die Spitze. Mit dem *Bundeswehrförderungsgesetz* werden, so der Autor Rolf Gössner, dessen Beitrag aus der Zeitschrift *Ossietzky* wir mit freundlicher Genehmigung abdrucken, bayerische Schulen, Hochschulen, Universitäten und Forschungseinrichtungen gesetzlich dazu angehalten, enger mit der Bundeswehr zu kooperieren. Das FIfF lehnt solche Bestrebungen zur Militarisierung bereits im Jugendalter entschieden ab und spricht sich nach wie vor für eine Zivilklausel an allen Hochschulen aus – zuletzt in der vorherigen Ausgabe, in der wir die *Frankfurter Erklärung* zur Zivilklausel abgedruckt haben⁴. Das dort abgedruckte Zitat von Wolfgang Borchert könnte auch als Motto des FIfF gelesen werden: „*Du, Forscher im Laboratorium. Wenn sie Dir morgen befehlen, Du sollst einen neuen Tod erfinden gegen das alte Leben, dann gibt es nur eins: Sag Nein!*“⁵

Eine eingehende philosophische Auseinandersetzung leistet Sarah Kessler zu dem Thema *Klima und KI – Vernunft ist nicht alles* – vielleicht eine Überlebensfrage der Menschheit und nicht erst seit dem Bestehen von *Bits & Bäume* ein zentrales Thema des FIfF. In ihrem Beitrag geht sie der Verbindung aus künstlicher Intelligenz und der Bestrebung nach sozial-ökologischer Nachhaltigkeit nach und versucht dabei, ein realistisches Subjektverständnis anzubieten. Der Beitrag erschien zunächst in *vorgänge – Zeitschrift für Bürgerrechte und Gesellschaftspolitik*.

Das 40-jährige Bestehen des FIfF haben wir in der Ausgabe 2/2024 der *FIfF-Kommunikation* gefeiert und werden dies bei der FIfF-Konferenz 2024 vom 25. bis 27. Oktober 2024 in Bremerhaven fortsetzen. Diese Ausgabe enthält ein Interview von *netzpolitik.org*, in dem Hans-Jörg Kreowski und Rainer Rehak ihre Sicht auf 40 Jahre FIfF, seine Erfolge und seine Zukunft darstellen. Weitere Beiträge zur Netzpolitik im Rahmen unserer Kooperation mit *netzpolitik.org* runden die Ausgabe ab.

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

Stefan Hügel
für die Redaktion



Anmerkungen

- 1 Erik Brynjolfsson (1993) *The Productivity Paradox of IT*: „computers are everywhere except in the productivity statistics“. Der Satz wurde inspiriert durch ein Statement von Robert Solow: „You can see the computer age everywhere but in the productivity statistics.“ Deswegen wird es gelegentlich auch Solow-Paradox genannt (https://en.wikipedia.org/wiki/Productivity_paradox).
- 2 <https://fragdenstaat.de/dokumente/249679-antrag-entwurf-der-fraktionen-der-spd-cdu-csu-buendnis-90-die-gruenen-und-fdp>
- 3 *Wir erinnern uns an den rechtsradikalen Mordanschlag von Solingen 1993, bei dem wenige Tage nach der Verabschiedung des „Asylkompromisses“ im Deutschen Bundestag fünf Menschen den Tod fanden.*
- 4 *Frankfurter Erklärung (2024) Kriegstüchtig? Friedensfähig! FfF-Kommunikation 41 (2), S. 13-14*
- 5 *Selbstverständlich muss sich dieser Appell auch an die Forscherinnen und wäre entsprechend anzupassen.*

Der Brief

... damit der Traum nicht aus ist.

*Gibt es ein Land auf der Erde / wo der Traum Wirklichkeit ist?
Ich weiß es wirklich nicht.
Ich weiß nur eins – und da bin ich sicher –: Dieses Land ist es nicht!
(Ton Steine Scherben, Rio Reiser, „Der Traum ist aus“)*



Liebe Freundinnen und Freunde des FfF, liebe Mitglieder,

die öffentliche politische Debatte wird derzeit von zwei Themen beherrscht: Der Migration Schutzsuchender nach Deutschland, und von Kriegen in der Ukraine, in Gaza und im Libanon, und auch – in der deutschen Öffentlichkeit weniger präsent – im Jemen. Innenpolitisch beobachten wir einen besorgniserregend wachsenden Zuspruch zum Rechtspopulismus, nach den Landtagswahlen in Brandenburg, Sachsen und Thüringen, wo die Alternative für Deutschland (AfD) die Mandatsmehrheit erreicht hat (in Thüringen) oder nur knapp an zweiter Stelle lag (in Brandenburg und Sachsen).¹

„... es gab keine Angst und nichts zu verlieren ...“

Mit kritischen Worten zu den genannten Landtagswahlen leitet Bundeskanzler Olaf Scholz seine Rede² zur Debatte über den Haushalt des Bundeskanzlers und des Bundeskanzleramts ein³ und kritisiert die AfD scharf. Im Weiteren benennt er Zuwanderung und Migration als eine der großen Fragen für die Zukunft unseres Landes und weist zunächst auf die Bedeutung der Zuwanderung für den Erfolg unseres Landes hin. Doch dann kommt er auf die „irreguläre“ Migration⁴ zu sprechen. Stolz führt er die repressiven Maßnahmen seiner Regierung auf und brüstet sich damit, diese Maßnahmen auch umgesetzt, anstatt wie die Parteien in der Opposition nur gefordert zu haben: Verlängerung des Gewahrsams, Reduzierung des Rechtsbehelfs, Reduzierung der Leistungen, Erweiterung der Zahl der „sicheren“ Herkunftsländer. Kurz gesagt: Diese Regierung hat menschenfeindliche Maßnahmen nicht nur verlangt, sondern auch durchgeführt. Dass das den Rechten und Konservativen immer noch nicht genügt, zeigen die im Protokoll vermerkten Zwischenrufe. Als Fazit ist festzuhalten: Die politische „Mitte“ rückt immer mehr nach rechts – womöglich ein Ergebnis des Rechtspopulismus der AfD, aber auch davon, dass die Parteien der „Mitte“ immer mehr deren Narrativen und Forderungen nachgeben.⁵ Sehr deutlich wurde dies bereits im Oktober 2023, als Bundeskanzler Scholz mit grimmiger Miene auf dem Titel des Magazins *Der Spiegel*

abgebildet war und mit den Worten zitiert wurde: „Wir müssen endlich im großen Stil abschieben.“⁶ Dies sagte er zu einer Zeit, als das Unwort von der „Remigration“ die Runde machte und Zehntausende zu großen Demonstrationen gegen Rechtspopulismus auf die Straße brachte. Grenzen in Europa werden wieder geschlossen und damit eine großartige Errungenschaft der Europäischen Union infrage gestellt, der freie Reiseverkehr. Welcher Schaden hier gerade angerichtet wird, ist vielleicht überhaupt noch nicht abzusehen.

Eins ist klar: Wir müssen dem Rechtspopulismus und seinen antidemokratischen Auswüchsen entschieden entgegentreten. Aber wir werden ihn nicht besiegen, indem wir uns seine Forderungen zu Eigen machen.

Gleichzeitig fordert eine Initiative, ein Verbotsverfahren gegen die AfD anzustrengen.⁷ Das Komitee für Grundrechte und Demokratie setzt sich differenziert mit der Frage des richtigen Weges im politischen Umgang mit der AfD auseinander.^{8,9} Die Diskussion darüber ist notwendig. Ob dieses Mittel – vielleicht das letzte Mittel des demokratischen Rechtsstaats – angemessen ist, muss der weitere Verlauf der Debatte zeigen, auch beim FfF.

„... es gab keine Waffen und keine Kriege mehr ...“

„Der Krieg muss nach Russland getragen werden“, so forderte der CDU-Militärpolitiker Roderich Kiesewetter angesichts der Aggression Russlands in der Ukraine.¹⁰ Dies scheint nach dem Gegenangriff der ukrainischen Streitkräfte auf Kursk und Drohnenangriffe auf russischem Gebiet nun gelungen zu sein und damit eine weitere Stufe der Eskalation dieses Konflikts zu eröffnen. Selbstverständlich ist es legitim, mit Gegenangriffen auf den Angriff Russlands zu antworten – doch wie können wir diese Gewaltspirale durchbrechen? Mit immer weiter eskalierenden Waffenlieferungen? Ich habe da so meine Zweifel. Namhafte Politiker:innen, wie der ehemalige EU-Kommissar Günter Verheugen¹¹, der die Ent-

wicklung des Verhältnisses zu Russland und die Frage der Aufnahme der Ukraine teilweise als Akteur selbst miterlebt und -gestaltet hat, zeichnen ein differenziertes Bild des Ursprungs dieses Konfliktes und fordern zu einer Politik der Entspannung auf.

Gleichzeitig steigt anscheinend auch sonst die Akzeptanz militärischer Lösungen. Wer sich wie ich an die großen Demonstrationen der 1980er-Jahre gegen die *Nachrüstung* im Rahmen des *NATO-Doppelbeschlusses* erinnert¹², reibt sich verwundert die Augen, wie gerade die Stationierung neuer Mittelstreckenraketen, die gegen Russland gerichtet sind, anscheinend ohne größere öffentliche Debatte durchgesetzt und akzeptiert wird. Damals war die Stationierung der *Pershing-II*-Raketen und der *Cruise Missiles* noch mit einem Verhandlungsangebot verknüpft. Heute gibt es nicht einmal das. Eine weitere Eskalation der atomaren Rüstung – auch angesichts der kurzen Reaktionszeiten und der damit verbundenen, wieder steigenden Gefahr eines *Atomkrieges aus Versehen*¹³ ist unverantwortlich – selbstverständlich auf beiden Seiten. Sie steht in Verbindung mit der weiteren Akzeptanz des Militärischen in der deutschen Außenpolitik – ausgerechnet unter einer rot-grün-gelb geführten Bundesregierung.¹⁴ Ob die Militärpolitik auch bei der Wahlentscheidung in Brandenburg, Sachsen und Thüringen eine Rolle gespielt hat, ist wohl nicht leicht zu beantworten – eine Umfrage der *Tagesschau* zeigt eine deutliche Betonung dieser Frage bei Wähler:innen der BSW und unterdurchschnittliche Bedeutung bei der AfD.¹⁵

In das Gesamtbild einer zunehmend repressiven Politik passt dann auch die aktuelle Initiative des Bundesinnen- und -heimatministeriums zur heimlichen Durchsuchung von Wohnräumen und der biometrischen Fernidentifikation von Personen anhand von Bildern im Internet. An der KI-Verordnung der Europäischen Union wurde bereits kritisiert, dass dies dort nicht klar verboten wird. Hier wird es wirklich gefährlich: Neben den heute schon bestehenden Möglichkeiten des Missbrauchs eröffnet dies nicht nur der aktuellen, sondern auch einer denkbaren rechtsextremistisch beeinflussten Regierung weitgehende Möglichkeiten der Repression – auch gegen politische Gegner:innen. Sie führen zu dem Risiko, sich nicht mehr anonym im öffentlichen Raum bewegen zu können und gefährden damit eine zentrale Grundlage der Demokratie. Das FfF hat sich gemeinsam mit anderen Organisationen dem *Bündnis Gesichtserkennung stoppen* angeschlossen, das eine klare Abkehr von diesem Weg fordert und die Verantwortung betont, „undemokratischen Kräften keine Werkzeuge auf den Tisch zu legen, die diese missbrauchen können – und werden.“

„... das war das Paradies.“

Sehr geehrte Mitglieder der Bundesregierung, sehr geehrte Mitglieder des Deutschen Bundestages: Bitte sorgen Sie – mit den angemessenen demokratischen Mitteln – dafür, dass die deutsche und europäische Politik nicht vom Rechtspopulismus, vom Rechtsextremismus und vom Militarismus bestimmt wird, oder ihm politisch repressive Möglichkeiten verschafft – ob direkt oder indirekt. Das bedeutet in erster Linie, Rechtsextremismus politisch zu bekämpfen. Das ist Ihre Verantwortung, dafür wurden Sie gewählt. Damit der *Traum* nicht aus ist.

Mit FfFigen Grüßen
Stefan Hügel

Anmerkungen

- <https://www.wahlrecht.de/>
- Deutscher Bundestag (2024) *Stenografischer Bericht der 184. Sitzung, Plenarprotokoll 20/184*, S. 23852 A ff.
- „... die traditionell für eine Abrechnung der Opposition mit der Politik der Bundesregierung genutzt wird“, wie die Medien in ihrer Berichterstattung selten vergessen zu erwähnen.
- Pro Asyl weist auf die Problematik dieses Begriffs hin, der bereits 2017 von der AfD verwendet worden sei (<https://www.proasyl.de/news/der-begriff-irregulaere-migration-und-wie-er-zur-taeschung-eingesetzt-wird/>). Mittlerweile sprechen auch Vertreter:innen von Bündnis90/Die Grünen von „irregulärer Migration“ (z. B. <https://www.zeit.de/news/2023-11/13/kretschmann-wir-muessen-irregulaere-migration-begrenzen>) – nur ein Beispiel dafür, wie rechtspopulistische Narrative immer mehr im Mainstream hoffähig werden.
- Lesenswert zur Rede von Bundeskanzler Scholz auch die Kolumne auf Spiegel Online: Samira El Ouassil (2024) *Wettrüsten der Menschenfeinde*, <https://www.spiegel.de/kultur/rechtsruck-in-deutschland-wettruesten-der-menschenfeinde-kolumne-a-1a1170f7-fdcd-4f3c-a40a-486cdcaddebc>
- Der Spiegel 43/2023, Titelblatt und Interview mit Bundeskanzler Scholz, S. 16 ff.
- Die Initiative betreibt eine Web-Seite unter <https://afd-verbot.jetzt>. Welche Organisationen und Personen im Einzelnen hinter dieser Initiative stehen, ist dort (Stand: 16. September 2024) noch nicht erkennbar – lediglich der Bund der Verfolgten des Nazi-Regimes stellt offen ein Spendenkonto dafür zur Verfügung.
- Komitee für Grundrechte und Demokratie (2024) *Radikal demokratisch gegen den Faschismus? Reflexionen des Komitees für Grundrechte und Demokratie zu einem möglichen AfD-Verbotsverfahren*, https://www.grundrechtekomitee.de/fileadmin/user_upload/Pdf/Grundrechtekomitee_AfD-Verbotsdebatte_02-2024.pdf
- Komitee für Grundrechte und Demokratie (2024) *Die Entleerung von Antifaschismus. Zur linken Anrufung der „wehrhaften Demokratie“*, <https://www.grundrechtekomitee.de/details/die-entleerung-von-antifaschismus-zur-linken-anrufung-der-wehrhaften-demokratie>
- Florian Naumann (2024) „Krieg muss nach Russland getragen werden“: CDU-Experte fordert Eskalation – gegen den Worst Case, FR online, <https://www.fr.de/politik/ukraine-waffen-deutschland-forderungappell-kiesewetter-cdu-russland-krieg-putin-zr-92825380.html>
- Günter Verheugen, Petra Erler (2024) *Der lange Weg zum Krieg. Russland, die Ukraine und der Westen: Eskalation statt Entspannung*, München: Heyne-Verlag und Günter Verheugen (2023): *Ab wann nahm das Verhängnis seinen Lauf?, vorgänge. Zeitschrift für Bürgerrechte und Gesellschaftspolitik* Nr. 239/240 [61(3-4)], S. 7-17
- ... und die – nebenbei – die Rahmenbedingungen schufen, unter denen damals das FfF gegründet wurde ...
- <https://atomkrieg-aus-versehen.de>
- Stefan Hügel (2024) „Mach, was wirklich zählt!“, *Der Brief, FfF-Kommunikation* Band 41 (2), S. 4-5
- Das Umfrageergebnis der *Tagesschau* zur Frage „Der Krieg zwischen der Ukraine und Russland spielt bei meiner Wahlentscheidung die größte Rolle“ zeigt beispielsweise 5 % Zustimmung bei allen Parteien, 17 % Zustimmung beim BSW und 3 % Zustimmung bei der AfD: https://www.tagesschau.de/wahl/archiv/2024-09-01-LT-DE-TH/charts/umfrage-wahlentscheidend/chart_1734144.shtml



40. FfF-Konferenz vom 25. – 27. Oktober 2024 an der Hochschule Bremerhaven

Vom 25.-27. Oktober 2024 findet die diesjährige Konferenz #FfFKon2024 des Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung an der Hochschule Bremerhaven statt.

Die #FfFKon2024 widmet sich dem Thema

Nachhaltigkeit in der IT green coding – open source – green by IT

Der Fokus dieser Tagung soll darauf liegen, wie wir nachhaltigere Ansätze innerhalb der IT verfolgen können und welche Rolle Open-Source-Projekte dabei spielen.

Neben IT-Projekten, die das Erreichen von Nachhaltigkeitszielen unterstützen, geht es bei der #FfFKon2024 vor allem darum, wie Software und Hardware selbst nachhaltiger gestaltet werden können. Dies ist umso dringlicher, als digitale Technologien und Infrastrukturen für einen beträchtlichen Anteil der CO₂-Emissionen verantwortlich sind.

Wie kann also aus Sicht der Informatik einer Entwicklung entgegengewirkt werden, bei der Digitalisierung eher ein Teil des Problems als ein Teil der Lösung ist?

Ein Einsparen von Hardware-Ressourcen gelingt am besten durch ressourcen- und energieeffiziente Softwareprodukte, also durch „Software, die schonend mit Hardware-Ressourcen umgeht, energiesparsam und auf älterer Hardware lauffähig und langfristig updatefähig ist“, wie es in der Umweltpolitischen Digitalagenda des BMU im Zusammenhang mit dem Zertifikat *Blauer Engel* heißt (siehe dazu den Vortrag von Anna Zagorski, Umweltbundesamt, am Samstag Vormittag).

Wie kann Software so programmiert werden, dass sie sparsam mit Software- und Hardware-Ressourcen umgeht? Wie kann das Handwerkszeug für das sogenannte „Grüne Coden“ bereits in der Programmierausbildung vermittelt werden? Wie können digitale Infrastrukturen nachhaltig gestaltet werden? Welche Rolle kann dabei Open-Source-Software spielen, die sich ja durch Transparenz, Anpassbarkeit und Austauschbarkeit auszeichnet? Mit diesen Fragen beschäftigen sich drei Workshops am Samstag.

Die ökologischen und sozialen Folgen der Rohstoffgewinnung für digitale elektronische Geräte stellen ein weiteres Problem der Digitalisierung dar. Um den Bedarf an neuen Geräten und Komponenten zu reduzieren, werden daher in immer mehr Bereichen Richtlinien für Reparierbarkeit, Wiederverwertbarkeit, modulares Design u. ä. eingeführt.

Wie können repair-, share-, reuse-, refurbish-Ansätze bei Gestaltung und Nutzung digitaler Geräte etabliert werden? Auch zu diesen Fragen gibt es Projektbeispiele und Workshops am Samstag. Das Programm der #FfFKon2024 verspricht also interessante Beiträge u. a. von Vertreter:innen des Alfred-Wegener-Institutes, des Umweltbundesamtes, des Bundesamtes für Sicherheit in der Informationstechnik und von Greenpeace Deutschland. Aus der

Perspektive anderer Disziplinen findet am Samstag Abend ein Gespräch über Nachhaltigkeit und globale Gerechtigkeit mit der Ökonomin Friederike Spiecker und dem Nachhaltigkeits- und Friedensforscher Jürgen Scheffran statt.

Samstagnachmittag haben wir parallele Workshoptracks zu folgenden Themen im Angebot:

- sichere, souveräne und nachhaltige IT-Umgebungen
- Reuse – refurbish – repair
- Green by IT und OSS
- Digital-nachhaltige Ko-Transformation
- Nachhaltigkeit in der Lehre

Auch das FfF-Projekt *Sensorstation für umweltbezogene Citizen Science* und die FfF-AGs *Faire Computer* und *Cyberpeace* laden zu Diskussionen über die künftige Arbeit ein.

Aktuelle Informationen zu Programm und Anmeldung finden sich unter <https://2024.fiffkon.de/>.

Mit den verschiedenen Beiträgen und Workshops erhoffen wir uns Diskussionen darüber

- ob und wie durch Open-Source-Software der CO₂-Verbrauch von IT-Systemen reduziert werden kann,
- wie ökologisch und sozial nachhaltige Entwicklungsansätze in Open-Source-Projekte eingebracht werden können,
- inwiefern Open Source die Gestaltung digital souveräner und langlebiger Infrastrukturen in Unternehmen, (öffentlichen) Verwaltungen, Schulen und Hochschulen unterstützt,
- und wie wir als FfF ressourcensparsame (Open-Source-) Projekte stärken können.

Die Workshops und Arbeitsgruppen finden am Samstag statt.

Am Sonntag feiern wir den 40. FfF-Geburtstag mit kleinen Geburtstagsreden von Frieder Nake, Dagmar Boedicker und Christiane Floyd. Den Abschluss bildet die FfF-Mitgliederversammlung.

Wir freuen uns auf eine spannende Konferenz und laden Interessierte herzlich ein.

Karin Vosseberg, Ulrike Erb, Oliver Radfelder und Lars Fischer (Organisationskomitee)

Einladung zur Mitgliederversammlung 2024

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

Wir laden fristgerecht und satzungsgemäß zur ordentlichen Mitgliederversammlung 2024 ein.

Sie findet am Sonntag, den 27. Oktober 2024, ab 11:00 Uhr an der Hochschule Bremerhaven statt.

Vorläufige Tagesordnung

1. Begrüßung, Feststellung der Beschlussfähigkeit und Festlegung der Protokollführung
2. Beschlussfassung über die Tagesordnung, Geschäftsordnung und Wahlordnung
3. Bericht des Vorstands einschließlich Kassenbericht
4. Bericht der Kassenprüfer
5. Diskussion der Berichte
6. Entlastung des Vorstands
7. Neuwahl der Kassenprüfer
8. Diskussion über Ziele und Arbeit des FifF, aktuelle Themen, Verabschiedung von Stellungnahmen, Berichte aus den Regionalgruppen
9. Anträge an die Mitgliederversammlung
Anträge müssen schriftlich bis drei Wochen vor der Mitgliederversammlung bei der FifF-Geschäftsstelle eingegangen sein
10. Verschiedenes
11. Genehmigung des Beschlussprotokolls

gez. Stefan Hügel
für den Vorstand und die Geschäftsstelle des FifF

Hans-Jörg Kreowski, Aaron Lye und Margita Zallmann

Cyberpeace – Für Frieden, Freiheit und eine lebenswerte Welt

Die Cyberpeace-Kampagne wurde vor zehn Jahren gestartet als eine Reaktion auf Edward Snowdens Enthüllungen über die weltweite Überwachung der Telekommunikation. Ziel war und ist, aufzuzeigen, dass die eingesetzten Cybertechnologien nicht nur Freiheitsrechte beschneiden, sondern auch eine erhebliche militärische Dimension besitzen. In dem sehenswerten Erklär-film *Cyberpeace statt Cyberwar* von Alexander Lehmann und Lena Schall ist das eindrucksvoll beschrieben (unter <https://vimeo.com/216584485> und <https://youtu.be/St955HBD-7k> abrufbar). In den ersten Jahren sind zahlreiche Publikationen erschienen, viele Vorträge gehalten und eine Reihe von Veranstaltungen wie Workshops, Kryptopartys, Cyberpeace-Cafés und Cyberpeace-Foren durchgeführt worden (siehe <https://cyberpeace.fiff.de/Kampagne/Home/>).

Die Kampagne hat vor vier, fünf Jahren an Schwung verloren – nicht zuletzt dann auch durch die Corona-Pandemie. Da aber die Thematik nichts an Aktualität eingebüßt hat, sollte Cyberpeace wachgehalten werden, In den letzten zwei Jahren ist dafür einiges passiert: ein Cyberpeace-Workshop auf der FifF-Konferenz 2022 in Berlin und einer im Sommer 2023 in Bremen, ein Cyberpeace-bezogener Schwerpunkt *Wissenschaft für den Frieden* in der *FifF-Kommunikation* 4/2023 und ein starker Cyberpeace-Schwerpunkt auf der FifF-Konferenz im vorigen Jahr, wie er in der *FifF-Kommunikation* 1/2024 dokumentiert ist, sowie als besonderer Höhepunkt das Positionspapier zu *Targeted*

Killing in der *FifF-Kommunikation* 2/2024.

Das wurde alles begleitet von der Cyberpeace-Rubrik und einzelnen thematisch bezogenen Artikeln der *FifF-Kommunikation*.

Es bleibt allerdings weiterhin ungeklärt, wie und mit welcher Zielrichtung die Cyberpeace-Kampagne fortgeführt werden soll. Ein Vorschlag dazu ist, wieder eine Cyberpeace-Webseite einzurichten, die die laufenden Aktivitäten widerspiegelt. Was vielleicht auch Sinn machte, wäre eine Art *Task Force*, die inhaltlich und organisatorisch für Kontinuität sorgt.

Auf jeden Fall steht auf der FifF-Konferenz Cyberpeace wieder auf der Tagesordnung (<https://2024.fiffkon.de/>):

Cyberpeace-Workshop: InformatikerInnen für Frieden

Die Kritik an der engen Verflechtung von Informatik mit Rüstung, Militär und Krieg war vor 40 Jahren einer der wesentlichen Gründe, das FifF zu gründen und mit *InformatikerInnen für Frieden* im Namen zu verankern. Und auch heute gibt es eher noch mehr Gründe für diese Zielsetzung. Dazu gehört der



immer ausgeklügeltere Einsatz von I&K-Technologie, neuerdings verstärkt von KI bei der Entwicklung von Waffen und Militärstrategie. Tödliche Drohnen gibt es inzwischen in unübersehbarer Vielfalt, viele Staaten stellen sie her, mehr noch schaffen sie an und ihr Einsatz ist inzwischen nahezu alltäglich. Die Systeme zur gezielten Tötung sind an Perfidie kaum mehr zu überbieten. Die zunehmende Drohung mit Atomwaffeneinsatz verstärkt auch wieder die Gefahr eines Atomkriegs aus Versehen, weil Frühwarnsysteme falschen Alarm schlagen. Und was hinsichtlich der Anwendung von KI bei der Entwicklung eines neuen Kampfflugzeugs (FCAS = *Future Combat Air Systems*) durch

Deutschland, Frankreich und Spanien geplant ist, ist kostspielig und abgründig. Aber bei Informatiker:innen für Frieden geht es nicht nur um den Informatikbezug des Kriegsgeschäfts, sondern auch um die Forderung, laufende Kriege zu beenden und Friedensverhandlungen aufzunehmen, um Friedensfähigkeit statt Kriegstüchtigkeit, um eine Umkehr der Zeitenwende.

Im Cyberpeace-Workshop sollen diese Themen auf der Basis von 5- bis 10-minütigen Impulsen diskutiert werden. Wer beitragen möchte, melde sich bitte per E-Mail an kreo@fiff.de, lye@fiff.de oder zallmann@fiff.de.

1 Ein Blick in die Zukunft

M 1: Fiktive Darstellung eines Kriegs mit autonom handelnden Waffensystemen (erstellt von Künstlichen Intelligenz Midjourney)



M 2: Auszug aus einem offenen Brief von Wissenschaftlerinnen und Wissenschaftlern aus den Bereichen Künstliche Intelligenz und Robotik an Bundesregierung, Bundestag und Zivilgesellschaft (2021)

Eine Maschine „sieht“ einen Menschen nur als eine lange Liste aus Zahlen und „versteht“ den Wert eines Menschenlebens nicht. Sie kann die weitreichenden Auswirkungen ihrer „Entscheidungen“ nicht „begreifen“.
[...]

Wir appellieren daher [...]: Stoppen Sie die Bewaffnung von Drohnen für die Bundeswehr. Setzen Sie sich für einen sofortigen Stopp der Verbreitung von bewaffneten Drohnen und für eine Ächtung von bewaffneten Drohnen und autonomen Waffensystemen ein.

Eine KI-erzeugte Szene zum Horror künftiger KI-Kriege aus einer Aufgabe des Staatsinstituts für Schulqualität und Bildungsforschung in München für das Fach Politik und Gesellschaft an Bayerischen Gymnasien.

Gemeinsamer Appell

Drohender Schaden für die Demokratie

Gemeinsame Stellungnahme zur geplanten Resolution des Bundestages zum Schutz jüdischen Lebens in Deutschland – 29. August 2024

Kunst und Wissenschaft, Kulturinstitutionen und Hochschulen sind wesentliche Diskursräume der Demokratie und damit auch Orte zur Vorbeugung und Bekämpfung von Antisemitismus und jeder Form von Diskriminierung. Zahlreiche Institutionen, Künstler:innen, Wissenschaftler:innen und Einzelakteur:innen haben durch künstlerische, zivilgesellschaftliche und wissen-

schaftliche Projekte Brücken gebaut und Räume für Verhandlung und Meinungsbildung geschaffen. Strukturen und Arbeitsprozesse im Kultur- und Wissenschaftsbereich wurden in den vergangenen Jahren zunehmend selbstkritisch analysiert und diversitätsorientiert weiterentwickelt.

In diesem Sinne begrüßen wir die Initiative, demokratische Maßnahmen zur Bekämpfung von Antisemitismus sowie gegen jede Form von Diskriminierung auf den Weg zu bringen.

Die öffentlich gewordene Fassung der geplanten Resolution des Deutschen Bundestags *Nie wieder ist jetzt: Jüdisches Leben in Deutschland schützen, bewahren und stärken*¹ erfüllt uns jedoch mit großer Sorge. Nach ersten juristischen Einschätzungen kollidiert sie mit dem Grundgesetz, bringt eine mannigfaltige Rechtsunsicherheit, zweifelhafte Praktikabilität und die Gefahr der Diskriminierung mit sich. Durch die autoritative Verwendung der sehr weitreichenden und gleichzeitig unscharfen IHRA-Arbeitsdefinition als Regulierungsinstrument, sowie durch die unklare Frage faktischer Bindung einer Bundestags-Resolution, droht sie enorme Verunsicherung mit sich zu bringen und zum Verstummen jener Stimmen zu führen, die durch entsprechende Ansätze geschützt werden sollen. Ein immenser Schaden für unsere Demokratie wäre die Folge. Doch der Bekämpfung von Antisemitismus gebührt eine Resolution, die mit der demokratisch-freiheitlichen Grundordnung in Einklang steht.

Bereits der gescheiterte Versuch, in Berlin eine Antidiskriminierungsklausel einzuführen, hat durch Verfahren und Form der Klausel, wie unlängst durch eine Umfrage bestätigt, den Glauben in die Politik und an eine konstruktive Zusammenarbeit tief erschüttert und die bereits stattfindende Antidiskriminierungsarbeit um Jahre zurückgeworfen. In der inhaltlichen Arbeit der öffentlich-geförderten Institutionen hat durch die enorme Verunsicherung Selbstzensur massiv zugenommen, der internationale Imageverlust Deutschlands als Wirtschafts-, Kunst- und Wissenschaftsstandort ist ebenfalls gravierend.

Indem zahlreiche Expert:innenstimmen, darunter die namenhafter Jurist:innen, Antisemitismusforscher:innen und Diversitätsexpert:innen, offensichtlich übergangen oder ignoriert werden und zum bisherigen Entstehungsprozess der Resolution wenig Transparenz herrscht, entstehen zusätzliche Irritationen.

Unterzeichnende Organisationen

AG Politik des Netzwerks TanzRaumBerlin | Akademie der Künste, Berlin | Aktion Tanz Dachverband Tanz Deutschland | Deutsche Gesellschaft für Sozial- und Kulturanthropologie, der Vorstand | Deutsche Jazzunion | Die Jüdische Stimme für gerechten Frieden in Nahost e. V. | DISK – Initiative Bild & Ton | ensemble-netzwerk | European Media Art Festival | Fachgesellschaft DeKolonial | Fachgesellschaft Geschlechterstudien | Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF) e. V. | Forum Ziviler Friedensdienst | Genossenschaft Deutscher Bühnen-Angehöriger r.V. (Bühnengewerkschaft GDBA) | Humanistische Union | ISD (Initiative Schwarze Menschen in Deutschland) | ITI Zentrum Deutschland | Jewish Solidarity Collective | lit.COLOGNE | Migrationsrat | medico international | Rat für die Künste, Berlin | Spore Initiative | TANZKOMPLIZEN Berlin | transmediale, festival for art & digital culture in Berlin | Vorstand des Rates für Migration | Weltfriedensdienst | Palestinian Jewish Academics, Verein in Gründung | Pro Quote Bühne

... und viele weitere persönliche Unterzeichner:innen

Anmerkung

¹ <https://fragenstaat.de/dokumente/249679-antrag-entwurf-der-fraktionen-der-spd-cdu-csu-buendnis-90-die-gruenen-und-fdp>

Außerdem resultieren, wie auch bei möglichen Klauseln, nicht absehbare Konsequenzen: Wenn ein Schutz entstehen soll, muss transparent sein, in genau welchem Fall die Resolution greift, wer dies kontrolliert und entsprechende Konsequenzen zieht.

Welche Stelle soll die Einhaltung der Resolution in rechtsstaatlicher Form überprüfen und sicherstellen können? Wie wird die Einhaltung von Grundrechten (z. B. Kunst-, Wissenschafts- und Meinungsfreiheit) gewährleistet? Wie wird vermieden, dass Förderung künftig von grundgesetzlich geschützten politischen Anschauungen abhängig gemacht wird?

Und vor allem: Wie wird sichergestellt, dass nicht ein Kontrollsystem etabliert wird, das von antidemokratischen Kräften missbraucht werden kann?

Gerade bei einem solch immens wichtigen Thema muss eine fundierte, tragfähige und zielführende Strategie in Zusammenarbeit mit der Zivilgesellschaft, mit Kunst und Wissenschaft und aufbauend auf die vorhandene Sachkenntnis angestrebt werden.

Wir rufen daher die Bundestagsabgeordneten aller demokratischen Parteien dazu auf, die Resolution im gemeinsamen Dialog mit Vertreter:innen aus Kunst, Wissenschaft und Zivilgesellschaft zu überarbeiten und ihre Verabschiedung zumindest zu vertagen – um zeitnah gemeinsam und öffentlich zielführende Ansätze zu entwickeln, die unsere wertebasierte und freiheitliche Demokratie festigen und Deutschland als Kunst- und Wissenschaftsstandort stärken.

Wir möchten die Vertreter:innen aller Parteien aufrufen, einen entsprechenden Dialog zu initiieren, um gemeinsam mit Expert:innen und Verbänden in aller Offenheit zielführendere Lösungen zum Schutz der Vielfalt jüdischen Lebens in Deutschland zu entwickeln.

Biometrischer Überwachungsexzess der Bundesregierung

Die politischen Reaktionen auf den Anschlag in Solingen beinhalten nicht hilfreiche, aber gefährliche Überwachungsvorhaben

30. August 2024 – Das neue „Sicherheitspaket“ der Bundesregierung beinhaltet gefährliche Überwachungsvorhaben. Die geplante biometrische Erfassung von Gesichtsbildern aus dem Internet ist ein Angriff auf die Grundrechte aller – ohne klare Notwendigkeit oder Nutzen.

Die gestrige Vorstellung eines Überwachungspakets in Reaktion auf den Anschlag in Solingen markiert einen neuen Tiefpunkt im fortwährenden Abbau von Grundrechten. Die Ampel-Koalition möchte faktisch Anonymität beenden und uns alle immer und überall identifizierbar machen.

Biometrische Massenüberwachung

Ermittlungsbehörden sollen das Internet nach Gesichtsbildern durchforsten und diese Daten für biometrische Abgleiche nutzen dürfen. Dieser massive Überwachungsvorstoß zur Gesichtserkennung wird noch nicht einmal begründet.

Diese neue Befugnis sollen die Ermittlungsbehörden „unter Beachtung der KI-Verordnung“ und des Datenschutzes erhalten, schreibt die Bundesregierung in ihrem „Sicherheitspaket“-Papier. Beides ist nicht nur eine Selbstverständlichkeit, sondern auch ein Widerspruch: Die KI-Verordnung verbietet es im Prinzip¹, KI-Systeme zu nutzen, um Datenbanken für biometrische Gesichtserkennung durch das massenhafte ziellose Auslesen von Gesichtsfotos aus dem Netz zu erstellen oder zu erweitern.

Verkauft wird die neue biometrische Rundum-Überwachung jetzt als „Maßnahme gegen gewaltbereiten Islamismus“. Doch schon in dem vor zwei Wochen geleakten BMI-Referentenentwurf für ein neues BKA-Gesetz² ist die Idee weitreichender biometrischer Überwachung enthalten. Und zwar mit noch mehr biometrischen Daten, die aus dem Internet gesammelt werden sollen, etwa „Bewegungs-, Handlungs- oder Sprechmuster.“

Tür auf für Palantir und Konsorten

Zusätzlich sollen polizeiliche Daten automatisiert mit Software analysiert und sogar für das Testen und das Training von „KI-Anwendungen“ genutzt werden. Das bedeutet praktisch, dass der ganze Zoo polizeilicher Datenbanken nicht nur zusammengeführt werden soll, sondern die Daten in „KI-Anwendungen“ enden werden. Offenbar ignoriert die Bundesregierung die Fehleranfälligkeit und Risiken von KI und sitzt dem KI-Hype auf.

Wer annimmt, die Polizei sei bisher handlungsunfähig durch zu geringe Befugnisse und müsse daher neue vorgeblich „moderne“ Methoden nutzen dürfen, hat offenbar ein ganzes Jahrzehnt von ständig erweiterten Befugnissen verschlafen. Beschnitten wurden diese allenfalls durch Entscheidungen des Bundesverfassungsgerichts. Auch die Ampel will offenbar das ständige Erweitern der Befugnisse fortführen.

Anonymität ist kein Verbrechen

Die biometrischen Überwachungsmaßnahmen führen in eine dystopische Zukunft, in der niemand mehr anonym im öffentlichen Raum oder im Internet unterwegs sein kann.

Das Recht, sich frei und unbeobachtet bewegen zu können, ist essentiell für eine funktionierende Demokratie. Eine Gesellschaft, in der jede Bewegung erfasst und analysiert werden kann, führt zu Selbstzensur, Misstrauen und einem Klima der Angst. Dieser Überwachungsexzess ist ein direkter Angriff auf die Freiheit und die Grundrechte jeder einzelnen Person.

Die Ampel sollte ihren eigenen Koalitionsvertrag lesen und sich daran erinnern, wofür sie einmal angetreten ist: „Den Einsatz von biometrischer Erfassung zu Überwachungszwecken lehnen wir ab. Das Recht auf Anonymität sowohl im öffentlichen Raum als auch im Internet ist zu gewährleisten.“

Die Kehrtwende zur biometrischen Massenüberwachung soll sämtliche offen im Netz verfügbaren Fotos zum behördlichen Abgleich missbrauchen. Das betrifft viele Millionen Abgebildete und verändert unsere Gesellschaft nachhaltig zum Schlechteren.

Dank an den Chaos Computer Club

Diese Stellungnahme wurde inspiriert von der Stellungnahme des CCC³ zum Thema.

Referenzen

- Maßnahmenpaket der Bundesregierung nach dem Anschlag in Solingen: https://cdn.netzpolitik.org/wp-upload/2024/08/240829_BMI_BMJ_BMWK_Sicherheitspaket.pdf
- Geleakter BMI-Referentenentwurf für ein neues BKA-Gesetz von vor Solingen: <https://netzpolitik.org/2024/trojaner-biometrie-big-data-wir-veroeffentlichen-den-entwurf-zum-neuem-bka-gesetz/>
- Koalitionsvertrag der Ampel 2021: https://www.spd.de/fileadmin/Dokumente/Koalitionsvertrag/Koalitionsvertrag_2021-2025.pdf
- Kritik an der KI-Verordnung bezüglich biometrischer Massenüberwachung: <https://netzpolitik.org/2024/ki-verordnung-biometrische-masseneuberwachung-ohne-wenn-und-aber/>

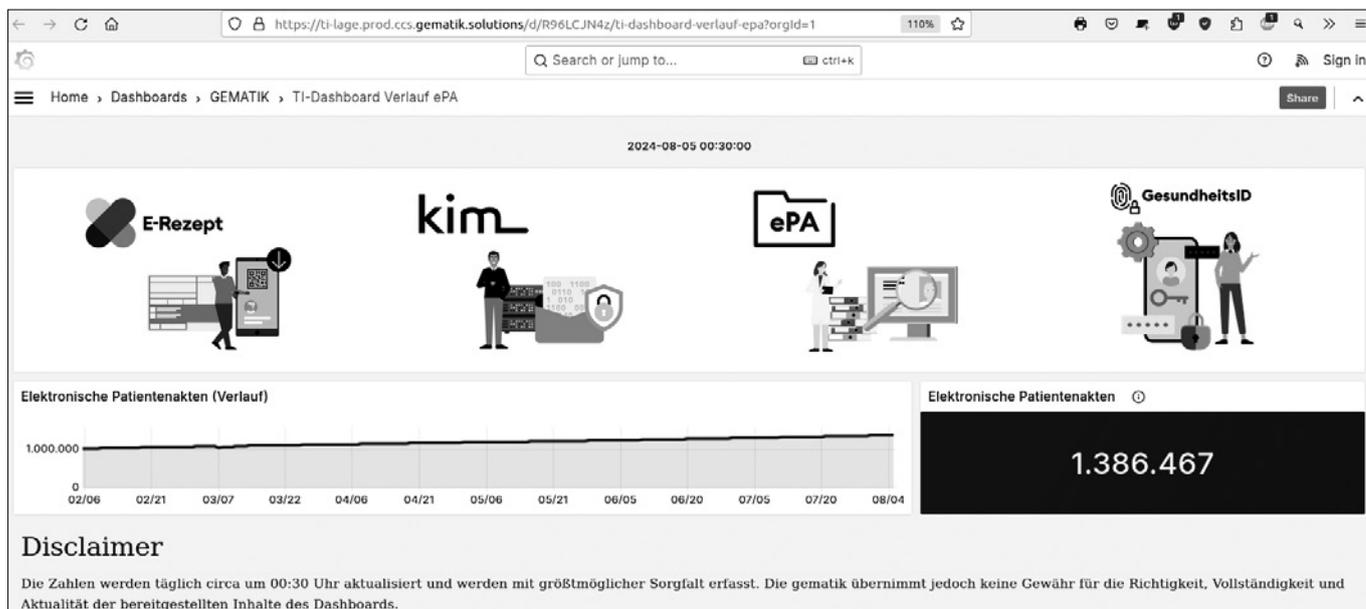
Anmerkungen

- <https://netzpolitik.org/2024/ki-verordnung-biometrische-masseneuberwachung-ohne-wenn-und-aber/>
- <https://netzpolitik.org/2024/trojaner-biometrie-big-data-wir-veroeffentlichen-den-entwurf-zum-neuem-bka-gesetz/>
- <https://www.ccc.de/de/updates/2024/biometrischer-uberwachungsexzess-der-bundesregierung>

Widerspruch gegen die elektronische Patientenakte (ePA)

Ein breites gesellschaftspolitisches Bündnis zur Verteidigung des Grundrechts auf informationelle Selbstbestimmung über die eigenen medizinischen Daten

Am 1. Januar 2021 wurde die elektronische Patientenakte, kurz ePA, eingeführt. Ab dem 15. Januar 2025 sind alle gesetzlichen Krankenkassen verpflichtet, für ihre Versicherten eine ePA anzulegen, sofern diese nicht widersprechen („Opt-out“). Bis zu diesem Datum richtet die Krankenkasse eine ePA nur auf Verlangen der Versicherten ein („Opt-in“).



Anzahl freigeschalteter ePAs

Quelle: Gematik – <https://ti-lage.prod.ccs.gematik.solutions/d/R96LCJN4z/ti-dashboard-verlauf-epa?orgId=1>

Die Nachfrage nach einer ePA war und ist bislang sehr gering. Mit Datum 5. August 2024 haben die gesetzlichen Krankenkassen auf Antrag der Versicherten 1.386.467 ePAs freigeschaltet (siehe Abbildung 1).

Da von den mehr als 84 Mio. Menschen in Deutschland rund 74 Mio. in der gesetzlichen Krankenversicherung (GKV) versichert sind, entspricht die Zahl der ePAs 1,87 % aller gesetzlich Versicherten. Wie viele davon ihre ePA im Kontakt mit Ärzt:innen, Psychotherapeut:innen und Krankenhäusern nutzen, ist nicht bekannt.

Ab Januar 2025: Von opt-in zu opt-out

Auf Grund von gesetzlichen Neuregelungen, die Ende 2023 vom Bundestag beschlossen wurden und im Februar 2025 mit Zustimmung des Bundesrats beschlossen werden sollen,

- erhalten ab 15. Januar 2025 zunächst in zwei Modellregionen (Franken und Hamburg) gesetzlich versicherte Menschen, die dem nicht widersprechen, automatisch eine solche ePA. Danach soll der Einsatz der ePA kurzfristig flächendeckend erfolgen. Dies gilt auch für alle nach diesem Zeitpunkt in Deutschland geborenen Kinder und – unabhängig von ihrer Staatsangehörigkeit – für alle nach diesem Zeitpunkt in die BRD einreisenden Menschen, sofern sie

nicht im Einzelfall privat krankenversichert sind oder Touristenstatus haben;

- außerdem sind alle Behandelnden verpflichtet, die ePA mit den Behandlungsdaten ihrer Patienten zu befüllen.

Die ePA wird als wichtiges Instrument zur Verbesserung der medizinischen Versorgung beworben. Sie hat aber mehrere gravierende Schwächen, die aus Sicht kritischer Versicherter, Ärzt:innen, Psychotherapeut:innen und Datenschützer:innen einen Widerspruch gegen die ePA notwendig machen, um die äußerst sensiblen persönlichen medizinischen Daten zu schützen. Sylvia Johnigk hat in der FfF-Kommunikation 2/2020 im Beitrag *Informationssicherheit und Datenschutz bleiben auf der Strecke bei der digitalen Transformation des Gesundheitswesens* (<https://www.fiff.de/publikationen/fiff-kommunikation/fk-2020/fk-2020-2/fk-2020-2-content/fk-2-20-p29.pdf> – dort S. 29 – 33) dazu umfangreich informiert.

Der Widerstand gegen opt-out formiert sich

Ende 2023 hat sich auf Initiative des Vereins Patientenrechte und Datenschutz e.V. (<https://patientenrechte-datenschutz.de/patientenrechte-und-datenschutz/ueber-uns/>) ein Bündnis von unterschiedlichen Gruppen und Personen gebildet, das über die Anfang 2025 in Kraft tretenden gesetzlichen Neuregelungen

und die Möglichkeiten des Widerspruchs gegen die elektronische Patientenakte (ePA) informiert.

Dem Bündnis gehören inzwischen mehrere ePA-kritische Vereinigungen von Ärzt:innen und Psychotherapeut:innen an, aber auch das Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung und weitere Organisationen und Einzelpersonen (<https://widerspruch-epa.de/buendnispartner/>).

Die in diesem Bündnis vertretenen Gruppen und Personen sehen durchaus, dass mit einer an den Interessen der Versicherten und der Behandelnden orientierten Digitalisierung im Gesundheitswesen ein individueller und gesellschaftlicher Mehrwert erzielt werden kann. Sie bewerten die gesetzlichen Neuregelungen aber kritisch, weil der Schutz von Gesundheits- und Behandlungsdaten durch die gesetzlichen Neuregelungen und die darauf basierenden technischen Lösungen nicht hinreichend gewährleistet ist. Dies wird u. a. daran festgemacht, dass die ePA nicht Patient:innen-zentriert umgesetzt werden soll; eine dezentrale Datenhaltung Missbrauch und Datenverlust reduzieren könnte; der Missbrauch medizinischer Daten durch Forscher:innen nicht hinreichend strafbewehrt ist und Regelungen für Entschädigungen bei Missbrauch oder Verlust von Daten fehlen.

Mit der Homepage <https://widerspruch-epa.de/> stellt das Bündnis umfangreiche Informationen (<https://widerspruch-epa.de/haeufig-gestellte-fragen-faq/>) zur Verfügung. Geplant ist zudem, Hilfestellungen (<https://widerspruch-epa.de/widerspruchs-generator/>) für die Formulierung von Widersprüchen anzubieten.

Was ist die ePA?

Die in der ePA gesammelten Informationen werden gesondert für jede gesetzliche Krankenkasse in zentralen Aktensystemen in der sogenannten Telematikinfrastruktur gespeichert. Dabei handelt es sich um eine digitale Infrastruktur zur Datenübermittlung/-speicherung im Gesundheitswesen. Diese wird im Auftrag der Krankenkassen von privaten Anbietern (IBM Deutschland, RISE / BITmarck, X-tention, InterComponentWare, ATOS und andere) betrieben. Dafür dürfen auch Cloud-Dienste, auch in den USA, genutzt werden. Aufgebaut und betrieben wird die Telematikinfrastruktur unter der Regie der gematik GmbH (Nationale Agentur für Digitale Medizin). Diese befindet sich mehrheitlich im Besitz des Bundesgesundheitsministeriums, daneben sind Verbände der Ärzte, Zahnärzte, Apotheken- und Krankenhausbetreiber usw. beteiligt.

Die ePA ist grundsätzlich als lebenslange Akte konzipiert. In der ePA sollen eine Vielzahl medizinischer Informationen über die jeweiligen Versicherten gesammelt werden, insbesondere

Befunde, Diagnosen, durchgeführte und geplante Therapiemaßnahmen, Vorsorgeuntersuchungen, Behandlungsberichte, Rezepte (Verordnungsdaten und Dispensierinformationen elektronischer Verordnungen), der Medikationsplan, Arztbriefe, der Mutterpass, eine Impfdokumentation, durch den Versicherten zur Verfügung gestellte Gesundheitsdaten, Daten von den Krankenkassen über in Anspruch genommene Leistungen, Bescheinigungen über Arbeitsunfähigkeit und anderes mehr. Für hochsensible Daten (zu psychischen Erkrankungen, sexuell übertragbaren Krankheiten und Schwangerschaftsabbrüchen) gilt, dass Patient:innen im unmittelbaren Behandlungskontext der Einstellung dieser Daten in die ePA widersprechen können, die Behandler:innen die Patient:innen auf das Recht zum Widerspruch hinweisen und den Widerspruch nachprüfbar in ihrer Behandlungsdokumentation protokollieren müssen. Für Ergebnisse von genetischen Untersuchungen oder Analysen im Sinne des Gendiagnostikgesetzes gilt, dass diese in der ePA nur gespeichert werden dürfen, wenn die Betroffenen explizit eingewilligt haben. Die Einwilligung muss ausdrücklich und schriftlich oder in elektronischer Form vorliegen.

Zugriffsberechtigungen auf die Daten in der ePA haben neben den Versicherten selbst Ärzt:innen, Zahnärzt:innen, Apotheker:innen, Psychotherapeuten:innen sowie deren jeweilige Mitarbeiter:innen inklusive Azubis; Altenpfleger:innen, Pflegefachkräfte, Kranken- und Altenpflegehelfer:innen; Hebammen, Heilmittelerbringer:innen (z. B. Physiotherapeut:innen, Logopäd:innen, Ergotherapeut:innen, Ernährungsberater:innen oder Podolog:innen) sowie deren jeweilige Mitarbeiter:innen inklusive Azubis; Ärzt:innen und Mitarbeiter:innen des Öffentlichen Gesundheitsdienstes, Fachärzt:innen für Arbeitsmedizin und Betriebsärzt:innen sowie Notfallsanitäter:innen.

Zusätzlich sollen die Daten an das Forschungsdatenzentrum Gesundheit (<https://www.forschungsdatenzentrum-gesundheit.de/>) weitergegeben werden, um sie interessierten und legitimierten Dritten (privatwirtschaftliche und universitäre Forschungseinrichtungen) in pseudonymisierter Form zur Verfügung zu stellen. Das FDZ ermöglicht bereits jetzt die Erschließung der Abrechnungsdaten aller gesetzlich versicherten Menschen in Deutschland, da es die Abrechnungsdaten jährlich in pseudonymisierter Form vom Spitzenverband Bund der Krankenkassen erhält. Vergleichbares gilt künftig auch für die in den ePAs gespeicherten Daten.

Was ist vor der Bereitstellung einer ePA zu beachten?

Jede gesetzliche Krankenkasse muss ausnahmslos alle ihre Versicherten über die gesetzliche Neuregelung informieren. § 343 Absatz 1a SGB V fordert, dass sie „den Versicherten, bevor sie

Walter Schmidt

Walter Schmidt, Frankfurt am Main, ist Mitglied des Vereins *Patientenrechte und Datenschutz e. V.*

ihnen eine elektronische Patientenakte... zur Verfügung stellen, umfassendes und geeignetes Informationsmaterial über die elektronische Patientenakte in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache und barrierefrei zur Verfügung zu stellen (haben) ...“ Danach haben alle Versicherten 6 Wochen Zeit, ihren Widerspruch gegen die ePA bei ihrer Krankenkasse anzumelden. Wer diese Frist versäumt, erhält danach eine ePA und alle behandelnden Ärzt:innen haben dann die gesetzliche Verpflichtung, die ePA mit ihren Behandlungen, Diagnosen, Medikationen, Röntgenbildern und was auch immer zu befüllen.

Aber auch danach haben alle Versicherten noch die Möglichkeit, wieder „auszusteigen“ und für die Zukunft die ePA abzulehnen und für die Vergangenheit die ePA komplett und unwiederbringlich löschen zu lassen. Was zu diesem Zeitpunkt aber bereits an das FDZ weiter gegeben wurde, ist nicht mehr zu löschen.

Worüber die Krankenkassen informieren müssen, ist in insgesamt 24 verschiedenen Punkten, die in §343 SGB V benannt sind, ausgeführt. Dort sind auch unterschiedliche Möglichkeiten des Widerspruchs gegen die ePA aufgelistet.

Was tun?

Das Bündnis Widerspruch gegen die elektronische Patientenakte (ePA) empfiehlt sowohl das vollständige Opt-out aus der ePA, als auch das Opt-out aus der Auswertung der Abrechnungsdaten durch die Krankenkassen für personalisierte Empfehlungen.

Für Versicherte, die der Bereitstellung einer ePA nicht widersprechen wollen, soll – so die bisherigen Planungen der gematik – ab 15. Juli 2025 die Möglichkeit für individuelle Freigaben oder Sperren für einzelne Dokumente, Bereiche oder Behandlungen sowie gegen die Weitergabe aller ePA-Daten für Forschungszwecke an das Forschungsdatenzentrum-Gesundheit bestehen.

Eine Beratung der Versicherten, die auch die Möglichkeit der Entscheidung für eine ePA offen lässt, wäre in unseren individualistischen Zeiten höchst wünschenswert. Einen Ansatz dafür gibt es von der Deutschen Aidshilfe (<https://www.aidshilfe.de/medien/md/epa/>).

Soweit einige Informationen zum Thema elektronische Patientenakte und zu den gesetzlichen Regelungen in der Bundesrepublik Deutschland.

Die geplante Verordnung der EU zum Europäischen Gesundheitsdatenraum

Der Europäische Gesundheitsdatenraum (EHDS, European Health Data Space) wurde nach Zustimmung der EU-Kommission und des EU-Ministerrats am 24. April 2024 vom EU-Parlament verabschiedet. Sie enthält teilweise vergleichbare, teilweise aber auch konträre Regelungen zu den gesetzlichen Regelungen in Deutschland, die einer gesonderten Bewertung unterzogen werden sollten.

Rolf Gössner

Militarisierung des Bildungssektors per Gesetz

Zum neuen bayerischen Bundeswehrförderungsgesetz und seinen fatalen Auswirkungen auf Universitäten, Hochschulen und Schulen

Militarisierung und „Kriegstüchtigkeit“ werden hierzulande seit Verkündung der sicherheitspolitischen „Zeitenwende“ nach dem russischen Angriff auf die Ukraine bekanntlich massiv forciert. Dabei sollen auch die Köpfe der mehrheitlich noch skeptischen Bürger und Bürgerinnen erobert werden – besonders die von Jugendlichen. „Wir müssen kriegstüchtig werden“, hat Bundesverteidigungsminister Boris Pistorius (SPD) wiederholt gefordert und damit nicht nur die Bundeswehr gemeint, sondern „unsere Gesellschaft“, also uns alle. Und so wird der Weg zu einer „wehrhaften“ Gesellschaft und einem „kriegstüchtigen“ Deutschland mit großem Aufwand politisch und ideologisch, medial und mental begleitet, unterstützt und gerechtfertigt. Erst kürzlich hat die bayerische Staatsregierung dabei einen weiteren Etappensieg erzielt: und zwar mit einer gesetzlich verordneten Militarisierung des staatlichen Bildungsbereichs.

Künftig werden bayerische Schulen, Hochschulen, Universitäten und Forschungseinrichtungen gesetzlich dazu angehalten, enger mit der Bundeswehr zu kooperieren. So regelt es das neue, bundesweit erste Bundeswehrförderungsgesetz, das der bayerische Landtag im Juli 2024 mit den Stimmen von CSU, Freien

Wählern und SPD beschlossen hat (LT-Drs. 19/1556; GVBl. Nr. 14 v. 20.07.2024, S. 257). Neben einem prinzipiell verordneten Kooperationsgebot wird auch ausdrücklich eine Kooperationspflicht der Hochschulen vorgeschrieben, wenn dies „im Interesse der nationalen Sicherheit erforderlich ist“.

Mit dem Gesetz soll eine „reibungslose Zusammenarbeit“ mit der Bundeswehr sichergestellt werden, außerdem ihr „ungehinderter Zugang“ zu Forschung und Entwicklung an Hochschulen, zu wissenschaftlichem Know-how und wissenschaftlich qualifizierten Fachkräften, so die Begründung. Im Gesetzestext heißt es wörtlich: „Erzielte Forschungsergebnisse dürfen auch für militärische Zwecke der Bundesrepublik Deutschland oder der Nato-Bündnispartner genutzt werden“ – demnach auch solcher Nato-Staaten, die Menschen- und Völkerrecht systematisch verletzen. Weiter heißt es im Gesetzestext: „Eine Beschränkung der Forschung auf zivile Nutzungen (Zivilklausel) ist unzulässig“. Denn, so die Begründung: Zivilklauseln seien „angesichts der bestehenden sicherheitspolitischen Herausforderungen nicht hinnehmbar“. Schließlich müsse das Forschungs- und Wissenschaftspotential bayerischer Hochschulen „auch

zugunsten militärischer Forschung und Entwicklung“ gesichert werden; und dazu gehöre auch, „Kooperationen oder Drittmitelprojekte mit Rüstungsunternehmen oder Armeen“ einzugehen und durchzuführen.

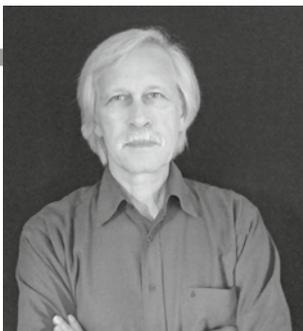
„Zivilklauseln“ sind bekanntlich Selbstverpflichtungen wissenschaftlicher Forschungseinrichtungen, ausschließlich für rein zivile und friedliche Zwecke zu forschen. Die grundgesetzlich verankerte Freiheit von Lehre und Forschung lässt eine solche freiwillige Beschränkung zu. Letztlich entstammt die zugrunde liegende Idee der Friedensbewegung der 1980er-Jahre; damit soll eine Politik der Abrüstung und Entspannung befördert werden, voll im Einklang mit dem „Friedensgebot“ des Grundgesetzes. Die erste Zivilklausel trat 1986 an der Universität Bremen in Kraft. Heute haben sie etwa 70 bundesdeutsche Universitäten und Hochschulen eingeführt – bislang jedoch keine bayrischen, denen dies nun für die Zukunft kategorisch verboten wird.

Auch alle Schulen in Bayern sind von dem Gesetz betroffen: Sie sollen von nun an im Rahmen der politischen Bildung zu „Fragen der Sicherheits- und Verteidigungspolitik“ eng mit „Jugendoffizieren“ und auch mit „Karriereberatern“ der Bundeswehr zusammenarbeiten – letztere im Rahmen schulischer Veranstaltungen zur „beruflichen Orientierung über Berufs- und Einsatzmöglichkeiten“ bei der Bundeswehr. Früher konnten Schulen und Lehrkräfte prinzipiell eigenverantwortlich entscheiden, ob und wie sie die Bundeswehr in den Sozialkundeunterricht einbinden. Allerdings referieren Jugendoffiziere der Bundeswehr bereits seit 1958 bundesweit vermehrt im Bildungsbereich über Sicherheitspolitik und Streitkräfte, häufig verbunden mit Truppenbesuchen. Seit 2008 sind Kooperationsvereinbarungen zwischen Bundeswehr und etlichen Bildungsministerien der Bundesländer geschlossen worden, die solche Bundeswehr-Besuche in Schulen verbindlich regeln. Unter Protest der Gewerkschaft Bildung und Wissenschaft (GEW), die den damit verbundenen zunehmenden Einfluss der Bundeswehr auf die inhaltliche Gestaltung des Unterrichts und der Lehreraus- und Fortbildung kritisiert. Politische Bildung gehöre „in die Hand der dafür ausgebildeten zivilen pädagogischen Fachleute“ und nicht in die von Jugendoffizieren. Schließlich gelte für Schulen das Gebot der Neutralität. Auch die Deutsche Friedensgesellschaft (DFG-VK) sowie die Deutsche Sektion der Internationalen Ärzt:innen für die Verhütung des Atomkrieges / Ärzt:innen in sozialer Verantwortung e. V. (IPPNW) halten die Öffnung des Schulunterrichts

für Programme der Bundeswehr für unvereinbar mit einer Erziehung zu Frieden, gewaltfreier Konfliktlösung und Völkerverständigung.

Tatsächlich ist die Bundeswehr weder verfassungsrechtlich noch nach den Bildungsgesetzen für politische Bildungsarbeit in Schulen legitimiert. Doch laut einem Gutachten der Wissenschaftlichen Dienste des Bundestages („Bundeswehr im Schulunterricht“, WD 3-09/10, 2010) sollen Informationen durch und über die Bundeswehr im Pflichtteil des Schulunterrichts verfassungsrechtlich grundsätzlich zulässig sein, weil „die Streitkräfte Teil des Staates und verfassungsrechtlich verankert sind“. Jugendoffiziere dürften aber nur auf Einladung der Schulen am Unterricht mitwirken und die Leitung der Informationsveranstaltung muss bei der Schule verbleiben. Je umstrittener die Inhalte in der Öffentlichkeit seien, desto eher müsse die Schule auf Ausgewogenheit achten und Gegenpositionen einbinden, wie etwa durch Vertreter oder Organisationen der Friedensbewegung (was häufig jedoch nicht passiert). Wegen der Verpflichtung zu Neutralität und Toleranz dürfe es keine gezielte Beeinflussung der Schüler in eine bestimmte Richtung geben (Indoktrinierungsverbot). Das gilt insbesondere auch hinsichtlich aktueller Kriegseinsätze bzw. militärischer Interventionen. Kontrovers debattierte gesellschaftliche Themen müssen kontrovers dargestellt und diskutiert werden. Und ein Werbeeffect für Militärdienst, also den Dienst an der Waffe, muss von vornherein verhindert werden – obwohl mit dem schulischen Einsatz von Jugendoffizieren ein solcher Effekt zumindest latent verbunden sein kann.

Mit dem neuen Bundeswehrförderungsgesetz werden solche begrenzenden Vorgaben praktisch obsolet, wird die Kooperation von bayrischen Schulen mit der Bundeswehr praktisch zum Zwang. Dies kann die Gewissensfreiheit von Schülern und Schülerinnen beeinträchtigen, wenn sie einseitig beeinflusst werden. Und es verstärkt, neben der damit verbundenen mentalen Militarisierung, einen bedenklichen Trend: Denn die Bundeswehr hat bereits in den letzten fünf Jahren bundesweit etwa 8.000 Minderjährige rekrutiert und an Waffen ausgebildet (mit Einverständnis der Erziehungsberechtigten); und dies mit zuletzt steigender Tendenz: allein 2023 waren es knapp 2.000, ein Rekordwert (taz 26.07.2024), und in Bayern sind fast 14 Prozent der Rekrutierten derartige Kindersoldaten. Und dies, obwohl der UN-Kinderrechtsausschuss ein Rekrutierungsalter von über 18 Jahren, also Volljährigkeit, fordert. Auch im Koalitionsvertrag der



Rolf Gössner

Dr. **Rolf Gössner** ist Publizist und Jurist, Kuratoriumsmitglied der Internationalen Liga für Menschenrechte sowie Mitherausgeber des jährlichen „Grundrechte-Report. Zur Lage der Bürger- und Menschenrechte in Deutschland“ und der Zweiwochenschrift für Politik/Kultur/Wirtschaft „Ossietzky“. Autor zahlreicher Bücher zu Demokratie, Innerer Sicherheit und Bürgerrechten, zuletzt: „Datenkraken im öffentlichen Dienst. ‚Laudatio‘ auf den präventiven Sicherheits- und Überwachungsstaat“, Köln 2021. Mehrfach ausgezeichnet, zuletzt mit dem Hans-Litten-Preis der Vereinigung Demokratischer Jurist:innen (VDJ).
Internet: www.rolf-goessner.de

Ampel steht, dass „Ausbildung und Dienst an der Waffe ... volljährigen Soldatinnen und Soldaten vorbehalten“ bleiben. Doch eine Umkehr ist bislang nicht in Sicht. Und so werden auch weiterhin Minderjährige, die sich durch Technik und Waffen, durch klare Ordnung, Kameradschaft und Abenteuer anfixen lassen, „kriegstüchtig“ gemacht – ganz besonders in Bayern.

Zum Sinn des Bundeswehrförderungsgesetzes heißt es in der Begründung: „Aufgabe des Staates“ sei es, „unsere Gesellschaft auf die grundlegend veränderte sicherheitspolitische Lage vorzubereiten“, die Auswirkungen auf fast alle Lebensbereiche habe. Auch der Freistaat müsse „im Rahmen seiner (Regelungs-) Kompetenzen dazu beitragen, die Bundeswehr zu stärken, die Rahmenbedingungen für die Erfüllung der Aufgaben der Bundeswehr ... bestmöglich auszugestalten sowie den Rückhalt in der Bevölkerung für unsere Soldatinnen und Soldaten zu festigen“. Dies ist jedoch keine bayerische Spezialität, sondern passt zum bundesweit staatlichen Bemühen, die Bundeswehr umfassend gesellschaftsfähig und uns alle „kriegstüchtig“ zu machen, was sehr viel mehr meint als grundgesetzkonforme Verteidigungsfähigkeit. Und tatsächlich gibt es längst Pläne des Bundesbildungsministeriums, das Militär bundesweit in Schulen noch intensiver informieren und werben zu lassen, um „ein unverkrampftes Verhältnis zur Bundeswehr“ zu entwickeln und Schüler „auf den Kriegsfall vorzubereiten“; und Hochschulen sollen nicht nur in Bayern, sondern bundesweit künftig stärker für Militär- und Rüstungsforschung geöffnet und dienstbar gemacht werden. Bayern bildet mit seinem Bundeswehrförderungsgesetz also die Vorhut, womöglich als Blaupause für die ganze Bundesrepublik.

Angesichts solcher Entwicklungen und Gefahren ist es gerade vor dem Hintergrund deutscher Geschichte mehr als angemessen, dass sich hiergegen organisierter Widerspruch regt. Und so warnten etwa DFG-VK, Gewerkschaften, Schul- und Hochschul-Angehörige und zahlreiche Personen des öffentlichen Lebens bereits im Vorfeld vor einer Verabschiedung des Gesetzes und kündigten eine verfassungsrechtliche Überprüfung an. Mehr als 1.500 Personen – darunter der Arbeitsrechtler Wolfgang Däubler, die Theologin Margot Käßmann, der ehemalige IG-Metall-Chef Jürgen Peters und der Liedermacher Konstantin Wecker – unterzeichneten eine Petition gegen das Gesetz, weil sie eine weitgehende „Militarisierung des Bildungs- und Forschungsbereichs“ befürchten – mit bundesweiter Ausstrahlung. Das Gesetz greife „unverhältnismäßig in die Autonomie der Hochschulen und damit in die Forschungs- und Wissenschaftsfreiheit ein“ und verstoße zudem gegen Neutralitätsgebot und Gewissensfreiheit an Schulen.

Aus all diesen Gründen muss der bayerische Verfassungsgerichtshof schnellstmöglich mit der verfassungsrechtlichen Überprüfung dieses Militärförderungsgesetzes und seiner mutmaßlich fatalen Auswirkungen befasst werden. Und die hoffentlich bald wieder gestärkte Friedensbewegung wird sich zusammen mit Gewerkschaften, Angehörigen des Bildungs- und Forschungswesens, Studenten, Schülern und Eltern dieser verhängnisvollen Angelegenheit und der zunehmenden gesellschaftlichen Militarisierung weiterhin mit Nachdruck annehmen und sich entschieden widersetzen müssen.



Sitz des bayerischen Verfassungsgerichtshofs im Neuen Justizgebäude in München, Foto: Christian Wolf, CC BY-SA 3.0

Hinweis: Der Autor ist Mitunterzeichner der Petition gegen das bayerische Bundeswehrförderungsgesetz; er wird deshalb auch eine baldige verfassungsgerichtliche Überprüfung unterstützen.

Der Beitrag erschien zuerst in Ossietzky. Zweiwochenschrift für Politik/Kultur/Wirtschaft Nr. 17/2024 vom 24. August 2024. Wir danken dem Autor und dem Verlag für die freundliche Genehmigung zum Nachdruck.

Referenzen

- Schulen und Wissenschaft müssen kooperieren. Bayern beschließt Bundeswehrgesetz: <https://www.lto.de/recht/nachrichten/n/bayern-bundeswehr-zivilklausel-kooperation-hochschulen-wissenschaftsfreiheit>
- Kritiker von Bayerns Bundeswehrgesetz drohen mit Klage: <https://www.sueddeutsche.de/bayern/bayern-bundeswehrgesetz-kritik-klage-lux-Tw2GeZXiz48UQgZFsMHgSo>
- Über 1.500 Personen unterstützen Petition gegen bayerisches Bundeswehrgesetz / Widerspruch gegen Gesetzesentwurf zur Militarisierung des Bildungsbereichs in Bayern: <https://www.gew-bayern.de/themen/nein-zumbundeswehrgesetz> <https://www.gew-bayern.de/aktuelles/detailseite/zum-gesetzesentwurf-zur-foerderung-der-bundeswehr-in-bayern> <https://www.gew-bayern.de/presse/detailseite/widerspruch-gegen-gesetzesentwurf-zurmilitarisierung-des-bildungsbereichs>
- Bayern macht Militarisierung zum Gesetz: Verbot von Zivilklauseln bei verstärkter Rekrutierung an Schulen: <https://www.labournet.de/branchen/dienstleistungen/bildung/bayern-macht-die-militarisierung-zum-gesetz-verbot-vonzivilklauseln-bei-verstaerkter-rekrutierung-an-schulen/>
- Gesetzesentwurf mit Begründung: <https://www.bayern.de/wp-content/uploads/2024/02/Entwurf-Gesetz-zur-Foerderung-der-Bundeswehr.pdf> / Bundeswehrförderungsgesetz im Bayerischen GVBl. Nr. 14 v. 20.07.2024, S. 257.

Klima und KI – Vernunft ist nicht alles

Das *irrational* (autonome) Subjekt sitzt mit am Tisch

Ende 2019 proklamierte die Europäische Kommission im Rahmen ihres neuen europäischen Green Deals eine sogenannte *duale Transformation* und betonte, dass die Bemühungen zur Dekarbonisierung und Digitalisierung Europas Hand in Hand gehen müssen. Doch was machen Dekarbonisierung und Digitalisierung mit dem autonomen Subjekt? Eine Reihe an Autor:innen diagnostizieren, dass das autonome Subjekt, im kantischen Sinne als vernünftig verstanden, seine beste Zeit hinter sich hat oder gar anachronistisch ist. Ein tatsächlich vernünftiges autonomes Subjekt war jedoch, so Sarah Kessler, von jeher eine Schimäre – deshalb ist auch die Diagnose des Anachronistischwerdens fehlgeleitet. In ihrem Beitrag geht Kessler der Verbindung aus künstlicher Intelligenz und der Bestrebung nach sozial-ökologischer Nachhaltigkeit nach und versucht dabei, ein realistisches Subjektverständnis anzubieten.

1. Intro

In der Ausgabe Nummer 242 der Zeitschrift *vorgänge* zum Schwerpunktthema künstliche Intelligenz (KI) haben Werner Koep-Kerstin und Philip Dingeldey ein Interview mit ChatGPT geführt. Darin haben sie den Chatbot auch zum Verhältnis zwischen KI und Nachhaltigkeit befragt. Mit diesem Verhältnis beschäftigt sich der vorliegende Beitrag. Genauer gesagt behandelt er die auf das spätmoderne Subjekt einwirkende Wechselwirkung der beiden jeweils mit der KI und der Nachhaltigkeit in Zusammenhang gebrachten „großen gesellschaftlichen Transformationen“ – also der erhofften Dekarbonisierung und Digitalisierung der Gesellschaft. Hier ein kurzer Ausschnitt des „Dialogs“ zwischen Mensch(en) und Maschine:

Das heißt, ChatGPT ist schädlich für das Klima?

ChatGPT an sich ist nicht schädlich für das Klima, da es eine Software ist und keine direkte Auswirkung auf die Umwelt hat. Allerdings erfordert die Nutzung von ChatGPT eine bestimmte Menge an Energie und Ressourcen, insbesondere wenn es auf großen Servern betrieben wird. Dieser Energieverbrauch kann sich auf die Umwelt auswirken, indem er CO₂-Emissionen verursacht, je nachdem, wie die Energie erzeugt wird. Es liegt jedoch auch an den Betreibern und Entwicklern, Maßnahmen zu ergreifen, um diesen Energieverbrauch zu minimieren und nachhaltigere Lösungen zu finden. (Koep-Kerstin/Dingeldey 2023: 119)

Besonders relevant für meine Überlegungen ist dieser letzte Satz. Der Chatbot weist die eigene Responsibilisierung zurück und scheint die Verantwortung für die CO₂-Emissionen stattdessen aufzuteilen und sie so teils der Technologienutzung und teils „den Betreibern und Entwicklern“ zuzuschreiben. In der Philosophie wird seit jeher dieser Zusammenhang zwischen *Verantwortung* und *Autonomie* diskutiert. Verantwortung kann nur tragen, wer autonom entscheidet. Wenn auch unterschiedliche ethische Traditionen dieses Verhältnis unterschiedlich zentral setzen, ist gerade im westlich modernen Verständnis¹ dieser Zusammenhang prominent verankert: *Wer die Wahl hat, hat die Verantwortung*. Das bedeutet, nur wer in der Lage ist, zwischen verschiedenen Optionen autonom zu entscheiden, dem kann die Verantwortung attestiert werden. Ergibt es dann Sinn zu fragen, ob der Chatbot klimaschädlich ist? Entscheidet er autonom? Was bedeutet überhaupt autonom? „[F]ür Kant [ist] ein

autonomes Leben nur durch von der Vernunft geleitete Gesetze und Regeln denkbar“ (Lindenau/Kressig 2023: 9; meine Herv.). Beschert die KI der Rationalität, mit der wir Entscheidungen treffen, eine neue Qualität? Trägt der Chatbot jetzt die Autonomie in unserer Gesellschaft? Die Debatte um KI kreist ständig um die Frage, ob Maschinen im Begriff sind, die Fähigkeit zur eigenen Zielsetzung zu entwickeln (*artificial general intelligence* – AGI) und vor allem, was derzeitige technologische Entwicklungen für einen Einfluss auf die menschliche Autonomie haben.

Wer die Wahl hat, hat die Verantwortung. Diesen Satz habe ich auch im Frühjahr 2019 kurz vor der damaligen Europawahl auf einem Plakat bei einer der ersten Fridays-for-Future-Demonstrationen in München gelesen. Die Wahl zu haben setzt weiterhin voraus, dass man über die Alternativen informiert ist, dass man über Wissen zu unterschiedlichen Parteiprogrammen und deren Positionierungen zu Nachhaltigkeitsaspekten verfügt und über das Wissen, welche politischen Maßnahmen als wirksam zu werten sind und welche womöglich eher propagiert werden, um den ökologischen Schein zu wahren. Um in Bezug auf die Klimafrage *vernünftig* abwägen zu können, ist Klimawissen unumgänglich. Dieses Spannungsverhältnis zwischen Vernunft, Autonomie und Verantwortung ist für beide erhoffte und politisch geforderte große Transformationen, um die es hier indirekt gehen soll, sowohl für die Dekarbonisierung als auch die Digitalisierung, entscheidend.

Um Transformationen beleuchten zu können, muss man sich sowohl die Ausgangslage als auch die Gegenwärtigkeit ansehen. Meadows et al. diagnostizierten bereits 1972 die *Limits to Growth*, weshalb ich, beginnend mit der ökologischen Frage, beim emanzipatorischen und ökologisch motivierten Aufbruchsgedanken der Neuen Sozialen Bewegungen der 1970er-Jahre ansetze. Hier diskutiere ich zunächst die Annahme, dass Autonomie, im Sinne Immanuel Kants auf individueller Vernunft basierend, im Laufe der *trente glorieuse*² durch flächendeckende Individualisierung und die daraus geborenen emanzipatorischen Neuen Sozialen Bewegungen zum *defining feature* der westlichen Moderne wurde.

Seither stach jedoch vor allem die dialektisch gewordene Qualität der Autonomie ins Auge – wir sahen „eher ‚erschöpfte‘ als autonome Subjekte“ (Rosa 2010: 200). Und mehr noch: „Die neuen Technologien des einundzwanzigsten Jahrhunderts könnten [...] die humanistische Revolution umkehren, indem sie die Menschen ihrer Autorität berauben und stattdessen nicht-

menschliche Algorithmen ermächtigen“ (Harari 2017). Heute wiederum, 300 Jahre nach Kant, beobachten wir also sogar vermehrt Diagnosen über „das Ende des autonomen Subjekts“ (Block/Dickel 2020: 110). Diese Diagnose will der vorliegende Aufsatz jedoch anzweifeln.

Um diese Diagnose zu widerlegen, gehe ich folgendermaßen vor: Der nächste Abschnitt (Abschnitt 2) beleuchtet zunächst noch etwas genauer die in der Soziologie viel debattierten Metamorphosen des autonomen Subjekts unter Bezugnahme auf das thematisierte Dreierverhältnis zwischen Vernunft, Autonomie und Verantwortung. Abschnitt 3 bespricht das autonome Subjekt im Zuge der ökologischen Frage. Er diskutiert die Diagnose der vermeintlichen Hegemonie der das autonome Subjekt auszeichnenden ökologischen Vernunft und Verantwortung in den (späten) 1970er-Jahren. Daraufhin beschäftigt sich Abschnitt 4 mit dem Einfluss der KI auf das autonome Subjekt. Anhand von Hartmut Rosas Resonanzkonzept diskutiert er die These, dass Selbiges jetzt in der Spätmoderne im Begriff ist, besonders aufgrund der momentanen Proliferation der KI, anachronistisch zu werden. Abschnitt 5 resümiert, dass die These des Anachronischwerdens des autonomen Subjekts auf einer zutiefst unvollständigen Konzeptionalisierung von Letzteren beruht. Versteht man das autonome Subjekt jedoch als kontingent und resonant, ist sie nicht plausibel. Das autonome Subjekt wird weder durch die fortdauernde Nicht-Nachhaltigkeit und das Ausbleiben ihrer allerorts geforderten Transformation, noch durch die die digitale Revolution revolutionierende KI anachronistisch.

2. Vernunft als Vorbedingung von Autonomie?

Um die Proklamation des vermeintlichen Endes des autonomen Subjekts in der Spätmoderne bewerten zu können, gilt es zunächst, seine bisherige Erfolgsgeschichte nachzuerzählen. In Kants Verständnis ist Autonomie durch Vernunft gegeben, für Kant ist Vernunft also Vorbedingung von Autonomie:

„Autonomie [ist die] Tauglichkeit der Maxime eines jeden guten Willens, sich selbst zum allgemeinen Gesetze zu machen, ist selbst das alleinige Gesetz, das sich der Wille eines jeden vernünftigen Wesens selbst auferlegt, ohne irgend eine Triebfeder und Interesse derselben als Grund unterzulegen.“ (Kant 1798: 95)

Obwohl es in Kants Verständnis neben der Vernunft weitere Faktoren gibt, die menschliches Handeln bestimmen, nämlich *Neigungen*, die „auf dem Gefühl der Lust und Unlust beruhen“ und den Menschen dadurch nur zu einem *teilvernünftigen* Wesen machen, sind diese jedoch nicht als Teil der menschlichen Autonomie gedacht, sondern vielmehr als Störfaktor. Kant versteht den Menschen als autonom, da er sich aus Vernunft *genötigt* sieht, sich einer subjektiven Neigung zu widersetzen und stattdessen autonom dem kategorischen Imperativ folgt – also seine Handlungsprinzipien selbst ableitet:

„Alle Gegenstände der Neigungen haben nur einen bedingten Werth; denn, wenn die Neigungen und darauf gegründeten Bedürfnisse nicht wären, so würde ihr Gegenstand ohne Werth sein. Die Neigungen selber aber, als Quellen der Bedürfnisse, haben so wenig einen ab-

soluten Werth, um sie selbst zu wünschen, daß vielmehr gänzlich davon frei zu sein, der allgemein Wunsch eines jeden vernünftigen Wesens sein muss.“ (Kant 1798: 64f.)

Ursprünglich war diese Befreiung von affektiven, irrationalen oder religiös bestimmten *Neigungen* und die Besinnung auf die jedem Menschen innewohnende, eigene Vernunft ein enormer emanzipatorischer Gewinn. Diese Kant'sche Norm der Autonomie erlebte jedoch erst in den 1970er-Jahren ihre wirkliche *time to shine*: „Autonomie war nun keine emanzipatorische Zielsetzung mehr, sondern Tagesordnung“ (Kalke 2024). Das *autonome Subjekt*, das *defining feature* des Projekts der Moderne schlechthin, emanzipierte sich also zunehmend aus den restriktiven Sicherheiten von Tradition und Zugehörigkeit und wurde im Laufe der *trente glorieuse* flächendeckend hegemonial, so lautet gemeinhin die Annahme (vgl. Rosa 2010; Staab 2022; Blühdorn 2020; 2024). Allen voran hat Ulrich Beck (1986) beschrieben, wie sich die transformativen, emanzipatorischen Neuen Sozialen Bewegungen als Antwort auf die fundamental neuartigen Herausforderungen der modernen globalen Weltordnung auf Kants Appell *sapere aude* rückbesinnt und somit Kants Hommage an die menschliche Vernunft in eine *reflexive Vernunft* und Notwendigkeit zur Übernahme von (ökologischer) Verantwortung übersetzt haben (vgl. auch Blanke 1986: 416).

Kommen wir nun zur Spätmoderne: *Wer die Wahl hat, hat die Verantwortung* – dieser Satz hat weiterhin eine für unsere *spätmoderne Situation* zentrale sowie konstituierende Bedeutung und weist nicht zuletzt auf das sogenannte *Paradox of Choice* hin: Dass dies aber nicht ausschließlich ein emanzipatorischer Gewinn, sondern im besten Fall ein zweiseitiges Schwert, im schlechtesten einen Pakt mit dem Teufel darstellt, steckt schon im Wort *Paradoxon*. Es gilt nicht nur: Wer die Wahl hat, hat die Verantwortung – obendrein haben wir auch noch die *Qual der Wahl*: Wer die Wahl hat, hat nicht nur die Verantwortung für die Informationsbeschaffung zur rationalen Abwägung der Alternativen, sondern auch noch die Verantwortung, ja sogar die Schuld, für *das Verpassen* der ausgeschlagenen Alternativen. Und hier ist es ganz egal, mit wie viel Vernunft sich das Subjekt das Hirn beim Abwägen der Alternativen zermartert hat.

Diese charakteristisch dialektische Interpretation der Entwicklung der westlichen Moderne, die ihre Wurzeln in der kritischen Theorie Max Horkheimers und Theodor W. Adornos hat und in Schriften wie Hans Jonas' *Das Prinzip Verantwortung* (1979) oder Robert Jungks *Der Atomstaat* (1977) Anwendung findet, scheint sich heute noch stärker zu bestätigen. Natürlich betrifft diese Entwicklung auch die Autonomie als Leitnorm. So unterstreicht beispielsweise Rosa das Verblässen des prophezeiten Freiheitsgewinns als Teil der abnehmenden Verheißungsqualität des Autonomieversprechens, während er auf der anderen Seite betont, dass es gleichzeitig in vielerlei Hinsicht so scheint als habe „die spätmoderne Gegenwartsgesellschaft [...] dieses [Autonomie-]Versprechen [...] in historisch einmaliger Weise eingelöst [...]: Subjekte können ihren Beruf, ihren Wohnort, ihren Lebensstil, ihre Religion, ja sogar ihren Stromanbieter, ihren Handytarif und ihre Krankenversicherung, an den äußersten Grenzen sogar ihr Geschlecht und ihren Körper, im Rahmen der Möglichkeiten ‚frei‘ wählen“ (Rosa 2010: 200).

Seit Neuestem sind diverse Autor:innen jedoch der Überzeugung, dass das charakteristisch moderne Verständnis von Autonomie in der Spätmoderne nicht mehr nur als ambivalent zu bewerten ist, sondern dass es zunehmend in Gänze verdrängt wird. Es ist also nicht mehr nur von einer Dialektik der Autonomie die Rede, sondern vielerorts sogar von ihrer Abschaffung: Philipp Staab (2022: 32) zufolge stellt die spätmoderne Gesellschaft momentan von einem Credo der Selbstentfaltung auf ein Leitmotiv der Selbsterhaltung um. So sei „die beobachtbare Demontage der Autonomie eine empirische Realität“, wie auch Katharina Block und Sascha Dickel (2020: 109; zit. & übers. n. Blühdorn 2024: 20) proklamieren. All diesen Autor:innen ist gemein, dass sie diese neueste Metamorphose der Autonomie mit der sich rasant entfaltenden Proliferation der KI in Verbindung bringen: So wertet Shoshana Zuboff (2019) die KI mit ihrer Fähigkeit des Datenscrapings und -analysierens sowie ihren darauf aufbauenden Möglichkeiten der Vorhersage, Zuschneidung und Manipulation von Nutzer:innen als fundamentale Bedrohung für die menschliche Autonomie und Selbstbestimmung. Block und Dickel (2020: 110) schreiben zudem, dass „im Rahmen eines in gesellschaftlichen Diskursen imaginierten und durch konkrete technische Installation vorangetriebenen Konzeptes einer algorithmisch gesteuerten Gesellschaft [...] die Idee eines humanistischen Subjekts als primären Quells sozialer Ordnung zunehmend anachronistisch [erscheint]“. Und Ingolfur Blühdorn (2024: 150) fügt hinzu: „Die digitale Revolution vollendet gewissermaßen die Ablösung des autonomen Subjekts als der modernistischen Zentralnorm“.

3. Die Unzulänglichkeit vernunftbasierter Autonomie für Nachhaltigkeitsbestrebungen

Ist diese Erzählung plausibel, dass das moderne, durch Vernunft ausgezeichnete, autonome Subjekt zu Zeiten der Neuen Sozialen Bewegungen breit gefordert wurde und diese Forderung heute anachronistisch wird? Wie oben beschrieben basiert Kants Autonomieverständnis auf universellen Prinzipien, die durch den Einsatz von Vernunft synthetisiert werden. Um jedoch bei solchen *allgemeingültigen* Prinzipien herauszukommen, muss das Kollektiv von vornherein mitgedacht werden – die Anderen sind im kategorischen Imperativ impliziert, er ist *relational*. Was aber nicht mehr mitgedacht wurde, ist, dass das Relationale nicht ausschließlich (oder vorrangig) als rational zu verstehen ist: Was hier also fehlt, ist das dem Relationalen innewohnende Nichtrationale, das Irrationale, das Unbegründbare, das Ungreifbare, das Unsichtbare, das Un(ter)bewusste, das Emotionale und Kulturelle.

Aber genau darin verbirgt sich das bisher überall verzweifelt gesuchte Puzzleteil, das das Paradox der *nachhaltigen Nicht-Nachhaltigkeit* (vgl. Blühdorn et al. 2020) auflösen kann³. Dieses oft identifizierte Paradox, die viel zitierte *value-action-gap* (vgl. Blake 1999), liegt nämlich genau in „[der] Gleichzeitigkeit eines nie dagewesenen Wissensstandes über – und öffentlichen Bewusstseins von – ökologische(n) und klimatische(n) Veränderungen, ihre(n) Ursachen und ihre(n) Auswirkungen einerseits und der entschiedenen Verteidigung von Strukturen und Lebensweisen andererseits, die bekanntermaßen ökologisch und sozial zerstörerisch sind“ (Blühdorn 2020: 66). *Die Auflösung verbirgt sich in der Einsicht, dass das Appellieren an ökologische Vernunft auf Basis von rationalen, faktenbasierten wis-*

senschaftlichen Erkenntnissen schon seit jeher zum Scheitern verurteilt ist, auch bereits zu Zeiten der Neuen Sozialen Bewegungen. Denn wie Gergen (1985: 270) schreibt, ist „Wissen [...] nicht etwas, das die Menschen in ihren Köpfen haben, sondern etwas, das die Menschen gemeinsam tun“. Wissenschaftliche Erkenntnisse sind zwar essenziell für den Umgang mit ökologischen Herausforderungen – der Trugschluss liegt aber in der Annahme, dass sie (fast) alles sind, worauf es ankommt. Hier schreibt Dan Sarewitz (2017): „[U]nserer Erwartungen an die aufklärerischen Ideale der angewandten Rationalität sind selbst irrational. Wir verlangen von der Wissenschaft das Unmögliche: Ein wissenschaftlich kohärentes und politisch vereinheitlichtes Verständnis von Problemen zu finden, die von Natur aus offen, unbestimmt und umstritten sind.“

Autonomie also rein oder auch nur hauptsächlich auf Vernunft basierend zu verstehen, ist daher reduktionistisch und in vielerlei Hinsicht fatal. Die Vernunftannahme (und mit ihr die Autonomieannahme im aufklärerischen Verständnis) wird nämlich schon allein davon untergraben, dass Menschen tatsächlich oft völlig *irrational* handeln, was jedoch aufgrund der Zentralität und des Stellenwerts des Rationalitätsanspruchs in moderner Politik und Wirtschaft gerne übersehen wird. John Maynard Keynes ([1936] 2018) war nach der Wirtschaftskrise der 1920er-Jahre bereits überzeugt, dass aufgrund omnipräsenter *Unsicherheit* vernunftbasiertes Abwägen überschätzt wird. Keynes folgt hier David Hume, der wiederum 1748 erkannte, dass wir, da wir nicht deduktiv bestimmen können, was wir nicht erleben, auf „Gewohnheit oder einen gewissen Instinkt unserer Natur [...] zurückgreifen müssen – Gewohnheit [...] ist der große Lotse menschlichen Lebens“ (Hume 1748). Es scheint fast in allen Teilen der Gesellschaft fraglich, ob ökologische Vernunft jemals in der Lage sein wird, die der Nicht-Nachhaltigkeit zu Grunde liegenden, in der Gesellschaft tief verwurzelten Gewohnheiten der spätmodernen Subjekte zu durchbrechen. War das zu Zeiten der Neuen Sozialen Bewegungen grundlegend anders? Herrschte damals das regulative Ideal der ökologischen Vernunft? Hier folge ich Daniel Hausknot (2017) in der Interpretation, dass auch damals keine weit internalisierte ökologische Vernunft vorlag. Eher würde ich sagen, dass die der Industrialisierung entspringenden Gewohnheiten nicht-nachhaltigen Handelns weniger lange und weniger umfangreich in der Gesellschaft verankert waren als sie es heute sind.

Da wir heute aber nun im *Zeitalter der Unsicherheit* (Bauman 2015) leben, das mit seinen immer schneller aufeinanderfolgenden Multikrisen eine Selbstverständlichkeit nach der anderen aushebelt, ist vernunftbasiertes Abwägen sogar noch aussichtsloser geworden. Rosa (2013) schreibt in diesem Zusammenhang, dass die Beschleunigung der modernen Welt die Autonomie der Subjekte untergraben kann, indem sie sie dazu zwingt, sich den Anforderungen der beschleunigten Welt anzupassen, anstatt gemäß ihren eigenen Werten und Überzeugungen zu handeln. Aber auch bereits zu Zeiten der Neuen Sozialen Bewegungen herrschte eine nie dagewesene, die damalige Situation erstmals charakterisierende Unsicherheit, die Beck überhaupt erst zum Anlass für sein berühmtes Buch *Die Risikogesellschaft* nahm. Rationales, vernunftbasiertes Handeln war bereits damals aufgrund der Neuartigkeit und vor allem neuerlichen Globalität der Risiken ähnlich heikel wie heute. Deshalb scheint es mir auch nicht plausibel, dass hier eine ökologische kollektive

Vernunft überhaupt gelten konnte, die das gute Leben für alle im Rahmen einer intakten Umwelt propagierte. Vielmehr waren die größtenteils lokalen ökologischen Gewinne damals politisch für die Aufrechterhaltung der staatlichen Legitimität notwendig, wie Hausknost (2017: 3) schreibt.

Blühdorn sieht den „Glaube[n] an unverhandelbare ökologische Imperative, ökologische Vernunft und Verantwortung“ als konstitutiv für die Hochzeit des öko-emanzipatorischen Projekts der 1970er und 1980er Jahre. Ökologische Vernunft ist jedoch viel komplexer, als es zunächst scheint: Die Erdsystemwissenschaft – man könnte sagen: die *Ausgeburt rationaler Vernunft* – liefert solide Erkenntnisse zum sich beschleunigenden und überall manifestierenden Klimawandel. Der Irrtum liegt jedoch in der Annahme, dass diese Erkenntnisse „nur noch“ in die Tat umgesetzt werden müssen und es hier politisch und gesellschaftlich rein gar nichts mehr zu diskutieren gibt (vgl. Blühdorn/Kessler 2023). Es gibt in Wahrheit bei Fragen rund um Heizungsgesetz und Tempolimit allerhand zu diskutieren, auch wenn die dazugehörigen wissenschaftlichen Erkenntnisse eindeutig sein mögen. Dass dieses „naturalistische Missverständnis“ (Beck 1988: 62), welches die Realität von gesellschaftlichen Begebenheiten und politischen Prozessen verkennt, von Beck bereits in den 1980er Jahren identifiziert wurde, deutet darauf hin, dass ein ökologischer Konsens auch damals nicht existierte. Auch damals machten sich solche Annahmen „des Vergessens von Gesellschaft schuldig“ (Beck 1988: 68). Auch damals gab es kein flächendeckend internalisiertes Ideal hinsichtlich ökologischer Vernunft und Verantwortung, und auch damals existierten gegenüber der ökologischen Frage fundamental unterschiedliche gesellschaftliche Standpunkte.

Ökologische Vernunft ist folglich, damals wie heute, als kulturell konstituiert⁴ und damit fundamental *kontingent* zu verstehen (vgl. Haderer 2021: 184) – ihr Imperativ ist nur einer unter vielen, und er ist mitnichten unstrittig, weder damals noch heute (letzteres belegen aktuelle empirische Untersuchungen zur gesellschaftlichen klimakulturellen Diversität; vgl. Kessler/Rau 2022; 2023; Kessler 2024). Außerdem treffen Menschen ihre Entscheidungen keineswegs hauptsächlich auf der Grundlage von rationalen Informationen – beispielsweise, weil einige davon nicht verfügbar sind und es unmöglich ist, alle Informationen zu verarbeiten, bevor eine Entscheidung getroffen werden muss. Gerade bei der ökologischen Vernunft ist es außerdem besonders problematisch, dass man äußerst oft mit *widersprüchlichen Informationen* konfrontiert ist – man denke nur an die berühmte Biogurke, die aber in Plastik verpackt zum Verkauf angeboten wird. Mit der modernen Rationalität hat das spätmoderne Subjekt auch darüber hinaus eine nicht eindeutige Beziehung – was es sich nicht gerne eingesteht: Man will als rational agierend, hinreichend wissenschaftlich bewandert und unemotional wahrgenommen werden und sich auf gar keinen Fall von irgendetwas „framen“ – lies: emotional manipulieren – lassen (vgl. Kessler 2024: 217). Der flächendeckende (spät-)moderne Appell an die Vernunft trägt jedoch selbst signifikant zur Aufrechterhaltung der Nicht-Nachhaltigkeit bei. Bisher waren Verantwortungszuschreibungen an das Individuum, grüner zu konsumieren, deswegen kaum erfolgreich, da sie nicht in der Lage waren, die Menschen *emotional* zu erreichen – eine Anforderung, die nicht nur die Zunft des Marketings, sondern auch die politische Neue Rechte schon lange erkannt und zu ihrem Vorteil genutzt haben.

Zur menschlichen Rationalität lässt sich zusammenfassend bisher Folgendes sagen: Sie ist weder immer das, worauf menschliches Handeln basiert, noch sollte man sich genau das wünschen⁵. Folglich ist es auch weder möglich noch sinnvoll, menschliche Autonomie rein auf Basis von *vernünftigem Abwägen* zu konzipieren: „Emotionen dienen als Klebstoff, der uns an Normen [und] die Ausübung gesellschaftlich sanktionierter Rollen [...] bindet“ (Ford/Norgaard 2019: 221). Vielleicht lässt sich der mangelnde Fortschritt beim Klimaschutz viel besser durch Nicht-Fühlen anstelle von Nicht-Wissen erklären, da der Fokus auf ökologische Vernunft die Bedeutung der affektiven, emotionalen und auch *körperlichen* Aspekte des Wissens ignoriert (vgl. Lidskog et al. 2020). Es gilt, Wissen stärker als *verkörpert* (im Englischen *embodied*) und nicht nur als rein kognitiv und zerebral zu verstehen. So betont Silvia Gherardi (2008: 517) in diesem Zusammenhang:

„Wissen ist nicht das, was im Kopf eines Menschen oder in Büchern oder Datenbanken steht. Wissen bedeutet, in der Lage zu sein, mit der erforderlichen Wissenskompetenz am komplexen Beziehungsgeflecht zwischen Menschen, materiellen Artefakten und Aktivitäten teilzunehmen. Aus dieser Definition folgt, dass Wissen in der Praxis immer eine praktische Leistung ist.“

Menschliches Handeln basiert außerdem zu einem erheblichen Teil auf Gewohnheit oder auf der Notwendigkeit, im Angesicht fundamentaler Unsicherheit *irgendwie nach vorne zu flüchten*, so dass wir manchmal, wenn wir „alle Rechtfertigungen erschöpft [...] und den Grundstein erreicht haben“, vielleicht einfach Wittgenstein (1953: 72) folgen und akzeptieren müssen, dass „dies einfach das ist, was ich tue“. Vollständig auf die Vernunft zu bauen, reduziert die Vernunft *ad absurdum*⁶, ist also bisweilen unvernünftig. Manchmal ist es vernünftig, irrational zu sein und einfach loszulegen, ohne jegliche Grundlage, denn es ist noch irrationaler, untätig zu bleiben, nur weil in manchen Fällen keine logische oder numerische Rechtfertigung geliefert werden kann. Wie könnten wir uns jemals zu etwas entschließen, wenn wir bei jeder Bewegung die Garantie bräuchten, dass dies auf jeden Fall das Beste ist, was wir tun können? Auch Keynes behauptete, dass die meisten alltäglichen Entscheidungen nicht von mathematischen oder gar vernünftigen Berechnungen abhängen, sondern von unserem angeborenen „spontanen Drang zum Handeln statt zum Nichthandeln“ ([1936] 2018: 141). Vielleicht ist es also gar nicht so falsch, aus einer Laune heraus zu wählen oder aus dem Instinkt heraus zu handeln? Die nützlichen Teile des unterbewussten Denkens sind vielleicht gerade durch natürliche Selektion erhalten geblieben.

Auf Basis dieser Überlegungen scheint es mir nicht plausibel, der Zeit der Neuen Sozialen Bewegungen einen Autonomiebegriff zuzuordnen, der auf einer damals vermeintlichen Hegemonie der ökologischen Rationalität und Verantwortung basiert. Es gibt erstens nicht *die eine* ökologische Vernunft – was sich nicht nur durch immer wieder auftauchendes und zurecht irritierendes widersprüchliches Wissen zeigt. Es zeigt sich auch durch die Tatsache, dass nicht nur diverse gesellschaftliche Gruppen eklatante klimakulturelle Unterschiede vorweisen, sondern wird auch darin deutlich, dass sogar unterschiedliche wissenschaftliche Disziplinen mit unterschiedlichen Rationalitäten operieren – sie sprechen sozusagen unterschiedliche Sprachen und daher

gerne aneinander vorbei. Zweitens, selbst wenn es eine ökologische Vernunft gäbe, würde diese nicht zwangsläufig in entsprechendem Handeln resultieren (vgl. Kessler 2024).

Nun theoretisiert Blühdorn, dass sich seit den Neuen Sozialen Bewegungen eine gesellschaftsweite *Emanzipation zweiter Ordnung* vollzogen hat, die im Abstreifen der Norm der vermeintlichen ökologischen Vernunft und Verantwortung besteht und so spätmoderne Autonomieansprüche rekonfiguriert. Diese Theorie der Autonomierekonfiguration setzt jedoch voraus, dass Autonomieansprüche über den Aspekt der Vernunft hinausgehen beziehungsweise etwas anderes als diese enthalten können.

Weiterhin ist aus meiner Sicht ein solches Verdrängen des spezifisch *modernen*, vernünftigen, autonomen Subjekts als zentraler Bezugspunkt der westlichen Moderne durch eine solche Emanzipation nicht überzeugend – denn es gab nie ein autonomes Subjekt, das dem Ideal der ökologischen Vernunft und Verantwortung entsprach. Versteht man die menschliche Autonomie jedoch von vornherein als *kontingent*, nämlich als kulturell beeinflusst und über das Kognitive hinausgehend, dann existiert es weiterhin.

4. KI kann aber nur Rationalität

Ist es nun jedoch plausibel, anzunehmen, dass „die digitale Revolution diese Ankernorm der Moderne [das vernunftbasierte autonome Subjekt] endgültig [verabschiedet] und [...] die künstliche Intelligenz an ihre Stelle [setzt]“ (Blühdorn 2024: 150)? Da „perfekte Rationalität eine Schimäre ist, weil niemand die geistigen Fähigkeiten besitzt, alle für eine schwierige Entscheidung relevanten Informationen in seinem Kopf zusammenzutragen“ (Matthews 1991: 114), müssen wir uns mit dem zufrieden geben, was *gut genug* ist. Herbert Simon ([1956] 1997) hatte dies mit seinem Konzept des *satisficing* angedeutet – die menschliche Rationalität ist notwendigerweise „begrenzt“ (*bounded rationality*), und zwar weil die *Rechenfähigkeiten* begrenzt sind: Wir können immer nur einen Bruchteil der tatsächlichen Informationen unserer Umgebung verarbeiten. Heben die digitale Revolution und die rapide fortschreitende Proliferation der KI diese Begrenzung der menschlichen Rechenfähigkeiten nun erstmalig auf?

In diesem Zusammenhang fordern Block und Dickel (2020: 126): „Die Soziologie sollte sich demnach Denkmöglichkeiten schaffen, das ‚Abseits‘ des autonomen Subjekts nicht nur als dystopisches Szenario zu befürchten oder resignativ als deterministische Folge von Technik hinzunehmen, sondern tatsächlich auch analytisch zu erschließen“. Befinden wir uns nun tatsächlich in einer trans- oder posthumanistischen Ära? Blühdorn widmet sich genau dieser Forderung von Block und Dickel und schreibt, dass die heutigen

„lernenden, voll kommunikationsfähigen Chatbots [in dem Weltwissen, auf das sie zurückgreifen, ihrem Tempo und meist auch in ihrer Artikulationsfähigkeit [...] natürlichen Personen längst überlegen [sind]. Spätestens seit der Markteinführung der ChatGPT-Software ist es irrational, ineffizient und unverantwortlich, bei der Bewältigung gängiger Aufgaben [...] nicht auf derartige Programme zurückzugreifen.“ (Blühdorn 2024: 149)

Mit dieser Annahme der (in Blühdorns Verständnis für das Subjekt *willkommenen*) Übertragung der menschlichen Autonomie auf die KI beschäftigt sich nun der folgende Abschnitt. Solch eine Übertragung ist jedoch nur konzeptionalisierbar, wenn man das autonome Subjekt rein auf kognitiver Vernunft basierend begreift. Versteht man es hingegen als kontingent, so wie von mir vorgeschlagen, lässt sich diese Diagnose nicht halten. Solch ein kontingentes Verständnis von menschlicher Autonomie entlarvt Blühdorns Diagnose als voreiligen *Anthropomorphismus*, denn die KI und Algorithmen sind mitnichten in der Lage, wirkliche, echte menschliche Autonomie (die eben über rationale Vernunft und individuelle Agency hinausgeht) zu ersetzen. Daher ist es auch nicht *irrational* oder *unverantwortlich*, auf sie zu verzichten. Oder man könnte sagen, dass wir es hier genau mit einem der Fälle zu tun haben, in dem es rational ist, das vermeintlich *Irrationale* zu tun und der KI, zumindest in manchen Situationen, zu entsagen. Weder die These, dass das autonome Subjekt in der spätmodernen Konstellation im Ringen um Nachhaltigkeit anachronistisch wird, noch, dass es die technologische Entwicklung der KI ist, die ihm den finalen Todesstoß versetzt, überzeugen letztendlich.

Aus meiner Sicht liegt bei der Frage, *ob das autonome Subjekt durch die KI anachronistisch wird*, die Krux eben in der oben in Zusammenhang mit der ökologischen Frage problematisierten Kant'schen Emporhebung der menschlichen Vernunft. So schreibt Blühdorn (2024: 144): „[...] [I]n der digitalen Gesellschaft sind als autonome Subjekte verstandene, natürliche Personen, denen nach modernistischer Tradition Vernunft und Moralität und eine unantastbare Würde zugesprochen wird, nicht mehr der relevante Bezugspunkt“. Sarah Spiekermann spricht in diesem Kontext von „der *klassischen* Unterscheidung von Vernunft und Intelligenz“ (Spiekermann 2020: 2; Herv. im Orig.). Mir scheint hier aber der Begriff der *Intuition* passender als der der *Intelligenz*. So soll das, was ich bisher als *kognitive Rationalität* oder *Vernunft* bezeichnet habe, dem Begriff *Vernunft* entsprechen und das, was ich als das dem Relationalen innewohnende Nichtrationale, das Irrationale, das Unbegründbare, das Ungreifbare, das Unsichtbare, das Un(ter)bewusste, das Emotionale und das Kulturelle beschreibe, als *Intuition* verstanden werden.

Nigel Thrift schreibt in diesem Zusammenhang, dass das menschliche Bewusstsein weitestgehend eine evolutionäre Sackgasse darstellt. Ihm zufolge hat die Forschung gezeigt, dass das Gehirn zum Großteil bereits vor dem Spracherwerb programmiert ist, was bedeutet, dass wir zu den meisten Gedanken keinen Zugang haben, weil sie unbewusst ablaufen. „Diese aufgewühlte Masse von Nervensalven bereitet den Körper so auf Handlungen vor, dass Absichten oder Entscheidungen getroffen werden, bevor das bewusste Ich sich ihrer überhaupt bewusst ist“ (Thrift 2007: 7). Nun basieren künstlich-intelligente Technologien wie ChatGPT auf *Large Language Models*, die allein auf Basis von Sprachprinzipien operieren – sie können also, wenn überhaupt, nur die sprachbezogenen und bewussten Aspekte der Fähigkeiten des autonomen Subjekts ersetzen: „Zumindest die bislang verfügbaren KI-Systeme verfügen nicht über die [für die menschliche Urteilspraxis] relevanten Fähigkeiten des Sinnverstehens, der Intentionalität und der Referenz auf eine außersprachliche Wirklichkeit“ (Deutscher Ethikrat 2023: 16). Zudem können sie menschliche Sprache niemals verstehen, sondern immer nur si-

mulieren: „Digitale Zustände und Prozesse *simulieren* mentale Zustände und Prozesse, sind aber nicht mit ihnen identisch, selbst wenn diese Simulation perfekt wäre. Nichts deutet darauf hin, dass mentale Zustände und Prozesse durch digitale Prozesse realisiert werden können. Simulation darf nicht mit Realisierung verwechselt werden“ (Nida-Rümelin/Weidenfeld 2022: 17).

Weiterhin können wir oft nicht exakt rekapitulieren, was wir im Austausch mit anderen gesagt haben, eher bleibt ein bestimmtes Gefühl, eine *Intuition*, zurück – das Gesagte (die Information selbst) bleibt nur schwer greifbar. Spiekermann bezieht sich dabei auf Bruno Bérard (2018), der schreibt:

„Wenn es in der Philosophie ein ‚vor und nach Immanuel Kant‘ (1724-1804) gibt, dann deshalb, weil er die Bedeutung von Intelligenz [SK: Intuition in meinem Verständnis] und Vernunft, wie sie von allen vorangegangenen Philosophen [...] verstanden wurde, auf den Kopf gestellt hat, da sie alle einer Illusion unterlagen, die nur er erkennen und auflösen konnte! Im Einklang mit seiner Überzeugung, dass Intelligenz [Intuition] nur vernünftig oder empirisch sein kann, erhob er die Vernunft in den höchsten Rang unter den kognitiven Fähigkeiten, die angeblich in der Lage sind, synthetische, systematische, universelle und vereinheitlichte Intelligenz zu liefern. Daher wurde die Intelligenz [...] [Intuition] der Vernunft untergeordnet: Ein sekundäres Vermögen, das sich mit der Verarbeitung von Abstraktionen befasst, das Sinneserfahrung eine begriffliche Form verleiht und die daraus resultierenden Begriffe zu einer kohärenten Struktur verbindet – bis es schließlich zu diskursivem Wissen, also zur ‚Vernunft‘ wird.“

Spiekermann (2020: 3) betont auch, wie ich es oben in Zusammenhang mit der ökologischen Frage bereits getan habe, dass Intuition (die sie *Intelligenz* nennt) körperlich erlebt wird – in bestimmten (besonders in sozialen, relationalen) Situationen reagieren unsere Körper, indem sie beispielsweise schwitzen oder rot anlaufen:

„Menschliche Vernunft ist stets als verleiblichte Vernunft zu begreifen. Praktische Vernunft ist zudem nicht aus einer rein individualistischen Perspektive zu verstehen. Da jeder Mensch Teil einer sozialen Mitwelt und kulturellen Umgebung ist, die sich nachhaltig auf seine Sozialisation auswirkt, müssen auch überindividuelle kulturelle Faktoren in die Deutung der praktischen Vernunft einbezogen werden.“ (Deutscher Ethikrat 2023: 17)

Für meine Überlegungen besonders entscheidend ist, dass Spiekermann schreibt, dass Intuition (respektive Intelligenz) „– im Gegensatz zur Vernunft – in der klassischen Lehre als ‚*noûs*‘ bezeichnet wird; das gleiche Wort wie das französische ‚*nous*‘, was zu Deutsch ‚wir‘ heißt. Die geteilte Wortwurzel weist darauf hin, dass Intelligenz [Intuition] etwas mit *Gemeinschaftlichkeit* zu tun hat“ (Spiekermann 2020: 3; meine Herv.). Genau dieser Aspekt der Gemeinschaftlichkeit ist auch für meine Überlegungen im Rahmen der unterschiedlichen Klimakulturen in der spätmodernen Gesellschaft zentral. Man kann die beharrliche Nicht-Nachhaltigkeit nur erklären, wenn man ein solch deutlich breiteres,

geteilte und unterbewusste Elemente mit einschließendes Wissenskonzept (das aus Vernunft und Intuition besteht) anwendet und dieses gleichzeitig als fundamental kontingent versteht. Genau dieses Verständnis, das auf relationalem Wissen beruht, ist auch zentral für eine Analyse, die verstehen will, wie die digitale Revolution die spätmoderne Gesellschaft verändert. Spiekermann (2020: 3) schreibt weiter, dass man oft sagt, dass man mit etwas „nichts anfangen“ kann, wenn es eben genau nicht gelingt, mit jemandem, oder in Relation zu etwas, solch ein relationales Verständnis aufzubauen:

„Man meint damit, dass man keine Intuition hat, wie man mit der gegebenen Sache umgehen soll. Für das Verstehen des Unterschieds zwischen menschlicher und künstlicher Intelligenz scheint dieses „sich mit etwas verbinden“ zentral. Es ist konstitutiv für den Unterschied zwischen Vernunft und Intelligenz [SK: Intuition]: Die Vernunft zerlegt eine Sachlage völlig neutral in Einzelteile, analysiert diese nüchtern ohne körperliche Reaktion und trifft möglichst Punkt-für-Punkt nachvollziehbare Entscheidungen. Die Intelligenz [Intuition] hingegen erfordert, dass man sich mit einer Sache verbindet, dass man etwas mit ihr anfangen kann.“ (Spiekermann 2020: 96f.)

Rosa (2017) schreibt in diesem Zusammenhang, dass „das Autonomiekonzept [...] nur die eine Hälfte der Resonanz [sieht]. Das alleinige Streben nach Autonomie kann am Ende das gute Leben auch verhindern“. Deshalb plädiert er stattdessen für die Idee der *Resonanz*, denn sie verlangt „auf der anderen Seite auch, dass starke Werte im Sinne von Charles Taylor erfahren werden“ (Rosa 2017)⁷. Zwar hat Kant bestimmte Werte in seinem Autonomieverständnis bereits mitgedacht – seine Rationalität ist ja relational zu verstehen. Rosas Resonanzbegriff ist ebenfalls fundamental relational gedacht, nur geht dieser über (auf Basis von kognitiver Vernunft gewonnene) *universelle* Werte hinaus (er ist also ebenfalls als *kontingent* zu verstehen), indem er auch Aspekte umfasst, die schwer fassbar und emotional sind. Indem er die Intuition mitdenkt, schafft es Rosas Resonanzbegriff – im Gegensatz zu Blühdorns Autonomiebegriff – eben auch das Irrationale und Ungreifbare zu fassen.

Ein Beispiel dafür stellt die Resonanz gegenüber Kunstwerken dar: Ein Gemälde oder ein Musikstück kann bei Betrachtenden oder Zuhörerenden eine starke emotionale Reaktion hervorrufen, die schwer in rationale Worte zu fassen ist. Diese Resonanz beruht oft auf einem tieferen Verständnis oder einer intuitiven Verbindung mit dem Kunstwerk. Auch können bestimmte Naturerlebnisse oder spirituelle Erfahrungen eine tiefe Resonanz in uns hervorrufen, obwohl wir diese Erfahrungen nicht vollständig verstehen oder erklären können. Rosa betont, dass Resonanz und Autonomie sich gegenseitig stärken können: Resonanz ermöglicht es den Menschen, ihre eigenen Bedürfnisse und Wünsche besser zu verstehen und authentische Beziehungen zu ihrer Umwelt einzugehen, während Autonomie es ihnen ermöglicht, diese Beziehungen aktiv zu gestalten und gemäß ihren eigenen Überzeugungen zu handeln. In einer resonanten Umgebung können Individuen ein tieferes Verständnis für sich selbst und ihre Umwelt entwickeln, was es ihnen erleichtert, autonom zu handeln und ihr Leben nach ihren eigenen Vorstellungen zu gestalten. Gleichzeitig können autonome Handlungen dazu beitra-

gen, resonante Beziehungen zu fördern und zu vertiefen, indem sie es den Menschen ermöglichen, authentisch und aufrichtig auf andere zuzugehen und sich mit ihnen zu verbinden (vgl. Rosa 2016; 2018).

5. Nur vernunftbasierte Autonomie wird durch den Algorithmus anachronistisch

An dieser Stelle ist es wichtig, anzuerkennen, dass wir umgekehrt auch nicht nur einfach das Ergebnis von Sozialisierung und Erziehung sind, sondern wir sind „aktiv an der Bildung unseres Charakters beteiligt“ (Nida-Rümelin/Weidenfeld 2022: 22). „Natürlich sind Erfahrung und Gewohnheit wichtig für die Entwicklung von Tugenden. Aber der Mensch ist in der Lage, seine Überzeugungen zu ändern und bewusste Entscheidungen zu treffen, seine Einstellungen in Zukunft zu ändern“ (Nida-Rümelin/Weidenfeld 2022: 22). Im Gegensatz zur KI verändert sich unsere „Software“⁸ also mit der Zeit im Rahmen des Spannungsfelds von Intentionalität und Intuition. Besonders erstaunlich ist jedoch, dass sich sogar die menschliche „Hardware“ verändern kann, was neueste Forschung zur Neuroplastizität des menschlichen Gehirns zeigt: „Neuroplastizität bezieht sich auf die Fähigkeit des Gehirns, sich ‚neu zu erfinden‘, nämlich sich zu verändern und sich in einer anderen Form zu formen, als Anpassung an neue Erfahrungen. Unsere Gehirne können sich transformieren, um sich an die Umgebung anzupassen“ (Crăciun 2023: 122). Dass die rapide Weiterentwicklung der KI sie eines Tages so potent werden lässt, dass sie sich als starke KI vom Menschen löst und sich (lies: ihre Software und Hardware) ebenfalls selbst erfindet, ist in Technologiekreisen ein breit diskutiertes Szenario (vgl. Hügel 2023: 6-10), das auch Steven Hawking bereits vor zehn Jahren zu denken gab: „Sie würde sich eigenständig ablösen und sich immer schneller selbst re-designen“ (Hawking 2014). Für wie realistisch man diese Prophezeiung hält, muss jede:r selbst entscheiden.

Rosa betont, dass Resonanz nicht vollständig kontrollierbar ist und dass wir nicht immer vorhersagen können, was in uns resonieren wird. Man kann zwar bestimmte Bedingungen schaffen, die die Wahrscheinlichkeit von Resonanzerlebnissen erhöhen, aber letztendlich bleibt Resonanz eine offene und dynamische Beziehung zwischen dem Individuum und seiner Umwelt. Resonanz wird so zu einem vielschichtigen Konzept, das sowohl rationale als auch emotionale, bewusste und unbewusste Elemente umfasst. Resonanz kann auch auf implizites Wissen oder intuitive Einsichten zurückzuführen sein. Manchmal fühlen wir uns von etwas angezogen oder abgestoßen, ohne genau zu wissen, warum. Diese Resonanz kann sich auf unmittelbare und unvermittelbare Erfahrungen beziehen, die nicht immer durch rationale Analyse erklärt werden können. Resonanz bezeichnet für Rosa somit nicht nur eine rationale Zustimmung oder Übereinstimmung, sondern auch eine tiefe emotionale Verbundenheit und Resonanzfähigkeit gegenüber der das Subjekt umgebenden Welt⁹.

Rosas Resonanzkonzept ist folglich hilfreich, um den Unterschied zwischen menschlicher und künstlicher Intelligenz zu verdeutlichen: Menschliche Intelligenz inkludiert kognitive Vernunft ebenso wie relationale, resonanzbasierte Intuition. Algorithmen der KI können aber nur mathematische, numerische Kalkulationen vornehmen, ihnen fehlt die *Resonanzfähigkeit*. Deswegen

ist es auch nicht plausibel, dass das autonome Subjekt als Zentralnorm der westlichen Moderne aufgrund der digitalen Revolution und der Proliferation der KI anachronistisch wird. Denn diese Diagnose ist den beiden von Kate Crawford (2021: 4f.) identifizierten Mythen aufgefressen:

„Der erste Mythos ist, dass nicht-menschliche Systeme [...] als analog zum menschlichen Geist verstanden werden können. Diese Sichtweise geht davon aus, dass mit ausreichendem Training oder genügend Ressourcen eine menschenähnliche Intelligenz aus dem Nichts geschaffen werden kann, ohne die grundlegende Art und Weise zu berücksichtigen, in der Menschen verkörpert sind, in Beziehungen stehen und in größere Ökologien eingebunden sind. Der zweite Mythos besagt, dass Intelligenz etwas ist, das unabhängig von sozialen, kulturellen, historischen und politischen Kräften existiert, als wäre sie etwas Natürliches und von diesen getrennt.“

Dass die Resonanzfähigkeit aufgrund von *fortgesetzter Individualisierung* (Beck 1986), noch mehr aufgrund einer die Spätmoderne charakterisierende *Singularisierung* (Reckwitz 2017) abnimmt, mag stimmen. Dass die Digitalisierung und vor allem die Algorithmisierung im Zuge der Ausweitung von KI-Anwendungen diese Tendenzen nochmals verstärkt, mag ebenfalls stimmen:

„Kein Nutzer weiß, was er alles nicht angezeigt bekommt, und die systematische Ausblendung bestimmter Inhalte kann zu einer verzerrten Weltansicht führen, wie von den Metaphern der Filterblase und Echokammer beschrieben. Hierbei geht es nicht nur um politische Inhalte, sondern Ideologien und extreme Ansichten aller Art können zur Keimzelle einseitiger Informationsumgebungen werden.“ (Stark/Margin/Jürgens 2019: 305)

Unter dieser Abnahme der Resonanzfähigkeit eine Verminderung der menschlichen Autonomie zu verstehen, weist jedoch nur einmal mehr darauf hin, dass wahrhaftige menschliche Autonomie von vornherein als relational, kontingent und resonant konzeptionalisiert werden muss. Gemäß einem solchen Verständnis wird auch die Annahme von praktischer Äquivalenz zwischen der Autonomie von Mensch und Maschine implausibel. Die Überlegung, dass „künstliche Intelligenz [...] eine neue Variante von *evidenzbasiertem* Entscheiden, Verwalten und Regieren [ermöglicht]“ (Blühdorn 2024: 147; Herv. im Orig.), wird so hinfällig. Darüber hinaus ist solch angeblich objektives, evidenzbasiertes Entscheiden letztlich jedoch genauso eine Schimäre wie völlig rationale Vernunft. So unterstreicht Simon Lindgren (2023): „Die KI hat, wie andere Technologien auch, eine gewisse ideologische Macht, da ihre Aura der maschinellen Objektivität dazu beiträgt, (in der Tat ideologische) Auffassungen als unpolitisch, natürlich und objektiv darzustellen“. Auch in der Welt der KI ist die Wahrheit nicht objektiv oder evidenzbasiert, sie ist fundamental kontingent, sowie mit ihr auch die menschliche Autonomie.

Es mag zu guter Letzt auch stimmen, dass die omnipräsente Anforderung, sich im Privaten wie Professionellen Profile zu erstellen und diese permanent zu kuratieren, dazu führt, dass das autonome Subjekt noch stärker fragmentiert, noch weniger zen-

tralisiert und in sich gefestigt zurückbleibt. Dennoch lässt sich daraus nicht schlussfolgern, dass zu Zeiten der Neuen Sozialen Bewegungen ein gefestigte(re)s und autom(er)es Subjekt existierte, das heute, besonders aufgrund der KI und Algorithmisierung zerfällt (wie oben bei der ökologischen Frage gezeigt).

Die Digitalisierung singularisiert nicht nur, sie vernetzt auch. Wird die Autonomie des Subjekts nicht mehr nur *kontingent*, sondern darüber hinaus auch *resonant* verstanden, wird sie von der digitalen Revolution vielleicht sogar an manchen Stellen erweitert – und nicht ausschließlich zurückgedrängt. In dieser dialektischen Spannung liegt wohl, einmal mehr, die Krux. Kontingent und resonant verstanden wird das autonome Subjekt also nicht anachronistisch, weder durch die fortdauernde Nicht-Nachhaltigkeit und das Ausbleiben ihrer allerorts geforderten Transformation noch durch die digitale Revolution.

Der Beitrag erschien zuerst in der Zeitschrift **vorgänge** als: Kessler, Sarah (2024): *Nachhaltigkeit und künstliche Intelligenz: Das irrationale (autonome) Subjekt sitzt mit am Tisch, vorgänge. Zeitschrift für Bürgerrechte und Gesellschaftspolitik* Nr. 245/246 [63(1-2)], S. 117-134. Wir danken der Autorin und der Redaktion für die freundliche Genehmigung zum Nachdruck.

Referenzen

- Adorno, T. W./Horkheimer, M. [1941] 1997: *Dialektik der Aufklärung*, Berlin.
- Bauman, Z. 2015: „Die Zeit ist aus den Fugen“, in: *ORF* vom 19.11.2015; online verfügbar unter: <https://sciencev2.orf.at/stories/1764698/index.html>.
- Beck, U. 1986: *Risikogesellschaft*, Frankfurt am Main.
- Beck, U. 1988: Das naturalistische Mißverständnis der Ökologiebewegung. Umweltkritik als Gesellschaftskritik, in: Beck, U.: *Gegengifte. Die organisierte Unverantwortlichkeit*, Frankfurt am Main.
- Beck, U./Beck-Gernsheim, E. 1994: *Risikante Freiheiten: Individualisierung in modernen Gesellschaften*, Frankfurt am Main.
- Bérard, B. 2018: Unmasking „AI“, in: *The Philos-Sophia Initiative* vom 22.02.2018; online verfügbar unter: <https://philos-sophia.org/unmasking-ai/>.
- Blake, J. 1999: Overcoming the 'value-action gap' in environmental policy: Tensions between national policy and local experience, in: *Local Environment*, Jg. 3, H. 4, S. 257–278.
- Blanke, T. 1986: Autonomie und Demokratie, in: *Kritische Justiz*, Jg. 19, H. 4, S. 406-422.
- Block, K./Dickel, S. 2020: Jenseits der Autonomie: Die De/Problematisierung des Subjekts in Zeiten der Digitalisierung, in: *Behemoth: A Journal on Civilisation*, Jg. 13, H. 1, S. 109-131.
- Blühdorn, I. 2024: *Unhaltbarkeit. Auf dem Weg in eine andere Moderne*, Berlin.
- Blühdorn, I. et al. 2020: Nachhaltige Nicht-Nachhaltigkeit. Warum die ökologische Transformation der Gesellschaft nicht stattfindet, Bielefeld.
- Blühdorn, I./Kessler, S. 2023: Ökologische Wende und Soziale Frage, in: Caritas Schweiz (Hrsg.): *Sozialalmanach 2024*, Luzern, S. 129-142.
- Crăciun, I. C. 2023: Förderung der Entwicklung im mittleren und höheren Lebensalter, Cham. https://doi.org/10.1007/978-3-031-44679-5_6.
- Crafts, N./Tonio, G. (2012). Les Trente Glorieuses: From the Marshall Plan to the Oil Crisis, in: Stone, D. (Hrsg.): *The Oxford Handbook of Postwar European History*, online edition; <https://doi.org/10.1093/oxfordhb/9780199560981.013.0018>, aufgerufen am 10.06.2024.
- Crawford, K. 2021: *The atlas of AI: Power, politics, and the planetary costs of artificial intelligence*, New Haven.
- Deutscher Ethikrat 2023: *Mensch und Maschine – Herausforderungen durch Künstliche Intelligenz*. Stellungnahme, Berlin.
- Gherardi, S. 2008: *Introduction: The critical power of the practice lens*. London.
- Haderer, M. 2022: Does emancipation devour its children? Beyond a stalled dialectic of emancipation, in: *European Journal of Social Theory*, Jg. 25, H. 1, S. 172-188.
- Harari, Y. N. 2017: *Homo Deus – A Brief History of Tomorrow*, New York.
- Hausknost, D. 2017: There never was a categorical ecological imperative: a response to Ingolfur Blühdorn, in: *Global Discourse*, Jg. 7, H. 1, S. 62-65.
- Hügel, Stefan 2023: „Mein Leben wird ganz wunderbar“ – Chancen und Risiken der künstlichen Intelligenz, in: *vorgänge. Zeitschrift für Bürgerrechte und Gesellschaftspolitik*, Nr. 242 = Jg. 62, H. 2, S. 5-21.
- Hawking, S. 2014: Interview by BBC Technology Correspondent Rory Cellan-Jones. Stephen Hawking warns artificial intelligence could end mankind, in: *BBC* vom 02.12.2014; online abrufbar unter: <https://www.bbc.com/news/technology-30290540>.
- Hume, D. 1748: *An Enquiry concerning Human Understanding*, online abrufbar unter: <https://davidhume.org/texts/e/full>.
- Jonas, H. 1979: *Das Prinzip Verantwortung*, Frankfurt am Main.
- Jungk, R. 1977: *Der Atomstaat: Vom Fortschritt in die Unmenschlichkeit*, Reinbek.



Sarah Kessler

Dr. **Sarah Kessler** ist Sozialwissenschaftlerin am Institut für Gesellschaftswandel und Nachhaltigkeit der Wirtschaftsuniversität Wien. Sie promovierte in der Anthropogeographie an der Ludwig-Maximilians-Universität (LMU) München und arbeitet zu Themen aus den Bereichen Umweltsoziologie, Nachhaltigkeitsforschung, Sozialtheorie, sozialer Wandel und soziale Bewegungen. Derzeit beschäftigt sie sich zudem vor allem mit den gesellschaftlichen Auswirkungen von künstlicher Intelligenz und deren Interrelation mit Nachhaltigkeitsfragen. Im März 2024 ist ihr Buch *Competing Climate Cultures in Germany* bei transcript erschienen.

- Kalke, K. 2024: Eine Frage der Autonomie, in: *makronom.de* vom 08.01.2024; <https://makronom.de/eine-frage-der-autonomie-45593>.
- Kant, Immanuel 1798: Grundlegung zur Metaphysik der Sitten, Original veröffentlicht von J. F. Hartknoch, online verfügbar unter: https://www.google.at/books/edition/Grundlegung_zur_Metaphysik_der_Sitten/f3MPAAAAQAAJ?hl=en&gbpv=0.
- Kessler, S./Rau, H. 2022: Capturing climate-cultural diversity: A comparison of climate change debates in Germany, in: Heimann, T. et al. (Hrsg.): *Climate Cultures in Europe and North America*, New York, S. 49-70.
- Kessler, S./Rau, H. 2023: Worte ohne Taten? Die Kluft zwischen Verantwortung und Wirksamkeit als Dilemma der Nachhaltigkeit, in Henkel, A./Gruber, H. (Hrsg.): *Dilemmata der Nachhaltigkeit*, Baden-Baden, S. 127-149.
- Kessler, S. 2024: Competing Climate Cultures in Germany: Variations in the Collective Denying of Responsibility and Efficacy, Bielefeld.
- Keynes, J. M. [1936] 2018: *The General Theory of Employment, Interest and Money*, Cambridge.
- Koep-Kerstin, Werner/Dingeldey, Philip 2023: Zwischen Falschinformation, menschenrechtlichen Problemen und kreativer Denkleistung. Ein Interview mit dem Chatprogramm ChatGPT, in: *vorgänge. Zeitschrift für Bürgerrechte und Gesellschaftspolitik* Nr. 242 = Jg. 62, H. 2, S. 107-119.
- Lidskog, R. et al. 2020: Cold science meets hot weather: Environmental threats, emotional messages and scientific storytelling, in: *Media and Communication*, Jg. 8, H. 1, S. 118-128.
- Lindenau, M./Kressig, M. M. (Hrsg.) 2023: Autonomie: Maßstab, Ideal oder Illusion? Vadian Lectures, Bd. 9, Bielefeld.
- Lindgren, S. 2023: *Critical theory of AI*, Hoboken.
- Meadows, D. h. et al. 1972: *The Limits to Growth*, New Heaven.
- Matthews, R. 1991: Animal Spirits, Chapter 7, in: Meeks, G. T. (Hrsg.): *Thoughtful Economic Man: Essays on Rationality, Moral Rules and Benevolence*, Cambridge, S. 103-125.
- Nida-Rümelin, J./Weidenfeld, N. 2022: *Digital Humanism: For a Humane Transformation of Democracy, Economy and Culture in the Digital Age*, Cham.
- Reckwitz, A. 2017: *Die Gesellschaft der Singularitäten: Zum Strukturwandel der Moderne*, Berlin.
- Rosa, H. 2010: Autonomieerwartung und Authentizitätsanspruch: Das Versprechen der Aufklärung und die Orientierungskrise der Gegenwart, in: Breidbach, O./Rosa, H. (Hrsg.): *Laboratorium Aufklärung*, München, S. 199-216.
- Rosa, H. 2013: *Beschleunigung und Entfremdung: Entwurf einer kritischen Theorie spätmoderner Zeitlichkeit*, Berlin.
- Rosa, H. 2016: *Resonanz – Eine Soziologie der Weltbeziehung*, Berlin.
- Rosa, H. 2017: Das Grundbedürfnis nach Religion wird bleiben. Ein Gespräch mit dem Soziologen Hartmut Rosa, in: *Herder Korrespondenz Hefte*, H. 10; online verfügbar unter: <https://www.herder.de/hk/hefte/archiv/2017/10-2017/das-grundbeduerfnis-nach-religion-wird-bleiben-ein-gespraech-mit-dem-soziologen-hartmut-rosa/>.
- Rosa, H. 2018: Hartmut Rosa über Resonanz, in: *Die Presse* vom 17.03.2018.
- Sarewitz, D. 2017: Stop Treating Science Denial like a Disease, in: *The Guardian* vom 21.08.2017; online verfügbar unter: <https://www.theguardian.com/science/political-science/2017/aug/21/stop-treating-science-denial-like-a-disease>.
- Simon, H. A. 1956: Rational Choice and the Structure of the Environment, in: *Psychological Review*, Jg. 63, H. 2, S. 129–138. CiteSeerX 10.1.1.545.5116. doi:10.1037/h0042769. PMID 13310708. S2CID 8503301.
- Simon, H. A. 1997: *Models of bounded rationality: Empirically grounded economic reason*, Vol. 3, Cambridge
- Spiekermann, S. 2020: Zum Unterschied zwischen künstlicher und menschlicher Intelligenz und den ethischen Implikationen der Verwechslung, in: Österreichischer Rat für Forschung & Technologieentwicklung (Hrsg.): *Ethische Herausforderungen im Zeitalter des Digitalen Wandels*, Wien, S. 94-125.
- Staab, P. 2022: *Anpassung: Leitmotiv der nächsten Gesellschaft*, Berlin.
- Stark, B./Magin, M./Jürgens, P. 2019: Maßlos überschätzt. Ein Überblick über theoretische Annahmen und empirische Befunde zu Filterblasen und Echokammern, in: Eisenegger, M. et al. (Hrsg.): *Digitale Strukturwandel der Öffentlichkeit: Historische Verortung, Modelle und Konsequenzen*, Wiesbaden, S. 303-321.
- Thrift, N. 2007: *Non-Representational Theory, Space, Politics, Affect*, Milton Park.
- Wittgenstein, L. 1953: *Philosophical Investigations*, Oxford.
- Zuboff, S. 2019: *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, New York.

Anmerkungen

- 1 Abgesehen von einer geringen Abweichung im Konsequentialismus, zu dem auch der Utilitarismus gehört: Hier wird Verantwortung auch für unvorhergesehene Nebenfolgen zugeschrieben – für die man per Definition, also da sie unvorhergesehen sind, nicht die (autonome) Wahl getroffen haben kann.
- 2 Gemeint sind damit die ersten 30 Jahre nach dem zweiten Weltkrieg, aus denen auch das deutsche Wirtschaftswunder hervorging (vgl. Crafts/Toniolo 2012).
- 3 Vgl. zur nachhaltigen Nicht-Nachhaltigkeit und Unhaltbarkeit auch den Beitrag von Ingolfur Blühdorn in diesem Heft.
- 4 Dieses Argument habe ich an anderer Stelle (vgl. Kessler/Rau 2022; 2023; Kessler 2024) umfangreich erläutert.
- 5 Siehe beispielsweise die instrumentelle Rationalität während des NS-Regimes (Adorno/Horkheimer [1941] 1997).
- 6 Wie das Gedankenexperiment des Esels aus Buridan verdeutlicht: Ein Esel ist ebenso durstig wie hungrig und befindet sich zwischen einer Portion Hafer und einem Eimer Wasser. Unter perfekter und reiner Anwendung seiner Rationalität kann er sich beim besten Willen nicht entscheiden und stirbt letzten Endes (vgl. Bérard 2018).
- 7 Solche Werte spiegeln tiefere, überindividuelle (aber eben nicht universelle) Prinzipien und Überzeugungen wieder.
- 8 Mir ist bewusst, dass ich mit diesem Bild ebenfalls anthropomorphisiere, das nehme ich aber for the sake of argument in Kauf.
- 9 Ähnlich schreibt Spiekermann (2020: 109): „Die ganze aristotelische Tugendlehre beschäftigt sich mit dieser Thematik des Menschen, ein gesundes Maß zu halten und in der Art seiner Entscheidungen weder durch ein Zuviel noch ein Zuwenig negativ in seine Gruppe hinein zu wirken. Was ihn oder sie jedoch dazu motivieren kann, dieses Maß zu halten, ist die Verletzbarkeit; etwa von der eigenen Gruppe nicht anerkannt zu werden, ausgestoßen zu werden, allein zu sein. An genau dieser Stelle unterscheidet sich die gelebte menschliche ‚Autonomie‘ ganz maßgeblich von der ‚Autonomie‘ eines KI-Systems. Zweitens nämlich wird vor allem als Möglichkeit verstanden, nach eigenem Kalkül eine Aktion anzustoßen, ohne eine Bestätigung vom Operator einzuholen. Soziale Erwägungen spielen dabei für die Maschine keine Rolle, denn sie ist nicht verletzlich. Es ist ihr egal, ob sie keinen Strom mehr bekommt oder abgeschossen wird, denn die Idee des Todes ist ihr im menschlichen Sinne nicht vermittelbar.“

Gegen die unheilvolle Verflechtung von Informatik und Militär

Das Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung begleitet und kommentiert seit nun vierzig Jahren eine Fülle an Themen. Im Interview sprechen wir mit Hans-Jörg Kreowski und Rainer Rehak über Aktivismus, langlebige Mythen der Informatik und durch Technik ausgelöste gesellschaftliche Umwälzungsprozesse.

Es gibt ihn seit Juni 1984, den Verein *Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung*¹, kurz FIFF. Seit 40 Jahren haben die Mitglieder den Anspruch, über die tiefgreifende Verflechtung von Informatik und Militär aufzuklären und sich für eine Abrüstung der Informatik in militärischen Anwendungen zu engagieren.

Sie setzen aufkeimenden Technik-Mythen mit fachlich fundierten Beiträgen etwas entgegen. Sie warnen vor überbordender Überwachung, werfen einen kritischen Blick auf die Tech-Konzerne und deren Geschäftsmodelle und bewerten Alternativen. Sie helfen auch ganz praktisch, beispielsweise zur Umgehung von Zensurmaßnahmen².

Anlässlich des vierzigjährigen Bestehens des FIFF haben wir mit Hans-Jörg Kreowski und Rainer Rehak darüber gesprochen, welche Rolle die Informatik im Bereich des Militärs damals und heute spielt. Welche Themen werden aktuell diskutiert?

Das FIFF in mehr als drei Sätzen

Constanze Kurz: *Was ist das FIFF in drei Sätzen beschrieben für die Menschen, die noch nie etwas von der Organisation gehört haben?*

Hans-Jörg Kreowski: Technische Entwicklungen sind nicht automatisch zum Wohle der Menschheit³ – vielfach natürlich auch, aber nicht nur. Die technische Basis für den gigantischen gesellschaftlichen Umwälzungsprozess, in dem wir uns befinden, ist die Informations- und Kommunikationstechnik. Das FIFF versucht, den Vermittlungsprozess zwischen einer fachlich-technischen Seite und der Gesellschaft herzustellen und Fehlentwicklungen zu zeigen.

Constanze Kurz: *Ist das FIFF also vor allem ein Vermittler und Kommentator?*

Rainer Rehak: Ich würde es noch erweitern. Die Art, wie wir kommentieren, kann in Form von Vorträgen, Büchern bis hin zu EU-Konsultationen oder Sachverständigen-Auskünften in Parlamenten sein. Demnach sind wir beim FIFF nicht nur Kommentator:innen vom Seitenrand, sondern auch Teil der Entscheidungsfindung und der demokratischen Meinungsbildung.

Die zweite Seite unserer Aufgabe, wie es Hans-Jörg gesagt hat, besteht darin, über Fehlentwicklungen und Technikmythen aufzuklären. Dazu zählt, dass wir in beide Richtungen kommunizieren. Manchmal kann es sein, dass Kolleg:innen innerhalb der Informatik gar nicht mitbekommen, wenn ihre Technik für kritische Dinge eingesetzt wird.

Constanze Kurz: *Was macht das FIFF besonders?*

Rainer Rehak: Eine Stärke des FIFF ist, dass es Menschen mit Expertise verbindet, die sich für Gesellschaft und Technik interessieren.

Constanze Kurz: *Das FIFF trägt auch den Begriff Frieden im Namen. Was hat Frieden damit zu tun, sich im FIFF zu engagieren?*

Hans-Jörg Kreowski: Ich bin seit über fünfzig Jahren in einem sehr theoretisch-mathematischen Kontext wissenschaftlich tätig. Ich hatte aber von Anfang an den Anspruch, die gesellschaftlichen Auswirkungen von Wissenschaft mit im Blick zu haben. Konkret bedeutete das für mich, die unheilvolle Verflechtung von Informatik und Militär zu verstehen und einzuordnen.

Das Militär hat die Entwicklung von Softwaretechnik und Programmiersprachen sehr stark geprägt. Wir sehen bis heute einen enormen Einfluss des Militärs, etwa wenn es um Künstliche Intelligenz geht. In den 1990er-Jahren hat sich die Informatik teilweise zivil emanzipiert.

hekta: *Welche Mythen half das FIFF aufzudecken?*

Hans-Jörg Kreowski: Ein großer Mythos um die Informationstechnik herum ist der Glaube, dass man damit nahezu alles machen kann und Probleme beliebig und eigentlich völlig grenzenlos lösen könnte. Von der fachlichen Seite her sind die Möglichkeiten der Informationstechnik aber erstaunlich eingeschränkt. Viele Dinge, die man zum Beispiel mit Datenverarbeitung machen und die man programmieren könnte, brauchen viel zu viel Zeit, als dass man auf die Ergebnisse warten kann. Das ist schon eine einfache technische Grenze, die sich bis heute überhaupt nicht verschieben lässt.

Oder nehmen wir den Mythos, dass Intelligenz so programmiert werden könne, dass Maschinen besser denken als Menschen. Bei allem, was ich über die Informatik weiß, gibt es kein Programm, das in der Lage wäre, selbständig zu denken. Dahinter stecken immer noch die Programme, die von Beginn an in der Informationstechnik geschrieben wurden.

Constanze Kurz: *In der Zeitschrift des FIFF geht es in der letzten Ausgabe auch um die kritische Einordnung des aktuellen KI-Hypes⁴. Welche Mythen sind denn wirklich gefährlich?*

Rainer Rehak: Es ist ein Mythos, dass Maschinen neutrale und objektive Ergebnisse liefern könnten. Daten oder ihre Verarbeitung sind selber nicht objektiv. Es ist daher nicht vertretbar, KI-Systeme bei bestimmten Entscheidungsfindungen mit einzubeziehen. Damit meine ich solche Entscheidungen, die sich explizit auf die Lebensumstände von Menschen auswirken.

Nehmen wir einmal an, das KI-System entscheidet darüber, wer berechtigt ist, Sozialleistungen zu beziehen, welche Medikamente ein Mensch braucht oder auch welches militärische Ziel

angegriffen werden soll. Es gab in den Neunzigern auch mal Expertensysteme zur Beratung für medizinische Behandlungen. Allerdings gab es auch Probleme mit diesen Expertensystemen.

Das liegt daran, dass die Systeme immer kontextabhängige Antworten geben. Menschen und die ganze Welt sind aber viel zu komplex, als dass uns ein System etwas über sie erzählen könnte. Hingegen kann ich gut ein System einsetzen, was einigermaßen verlässlich meine Pflanzen gießt oder neue Musik vorschlägt, und wenn es mal nicht klappt, ist das auch nur mäßig schlimm.

Informatiker warnten vor programmiertem Atomkrieg

Constanze Kurz: *Wenn man auf die 40 Jahre Fiff blickt, dann ist vielleicht das Thema KI immer wieder präsent, aber nicht das Überthema, sondern nur eines von vielen. Was waren die Impulse in Bezug auf Friedensfragen, um das Fiff zu gründen?*

Hans-Jörg Kreowski: Da gehen wir jetzt deutlich über 40 Jahre in die Zeit zurück, wo noch über den NATO-Doppelbeschluss und die Aufstellung von rund 200 Atomsprengköpfen sowie mehreren hundert Marschflugkörpern verhandelt wurde. Sie waren als eine Abschreckung gegen die sowjetischen SS-20-Raketen gedacht. Wären sie zum Einsatz gekommen, wäre von Mitteleuropa und Deutschland nichts mehr übrig. Das war der Ausgangspunkt für eine riesige Friedensbewegung mit hunderttausenden Teilnehmenden. Das Fiff bildete sich eben aus dieser Friedensbewegung genauso wie etliche andere Friedensinitiativen.

hekta: *Und wer hat sich am Anfang besonders engagiert? Was waren das für Menschen?*

Hans-Jörg Kreowski: Die Friedensinitiativen aus den Universitäten waren ganz überwiegend Studierende, wissenschaftliche Mitarbeiter:innen, Professor:innen. Für die Gründung des Fiff waren natürlich die rund ein Dutzend Fachbereiche für Informatik entscheidend. Es gab aber auch Gewerkschaftsgruppen, die an der Gründungsversammlung teilgenommen haben.

hekta: *Wie haben sich die Fachleute aus der Informatik damals für ein gemeinsames Friedensziel eingebracht?*

Hans-Jörg Kreowski: Ein Thema waren die unzuverlässig programmierten Frühwarnsysteme. Das Risiko dieser Systeme bestand darin, dass sie fälschlicherweise Bedrohungen meldeten und damit leicht zu falschen Entscheidungen hätten führen können. Deshalb starteten die verschiedenen Initiativen auch eine gemeinsame Kampagne unter dem Motto „Informatiker warnen vor dem programmierten Atomkrieg“. Das war der Anfang.

hekta: *Womit beschäftigt sich das Fiff aktuell und warum?*

Rainer Rehak: An vielen Stellen fokussiert man sich auf Technik⁵, um bestimmte gesellschaftliche Missstände anzugehen. Man beschäftigt sich sehr viel mit Technik und fragt sich, welches die beste von allen⁶ ist und ob man sie kauft oder nicht. Leider wird dadurch weniger darüber geredet, wie man es vielleicht ohne Technik anders verbessern könnte. Es tritt komplett in Hintergrund, wofür diese Technik eigentlich sehr gut wäre und was ein

sinnvoller und bedürfnisorientierter, auch kontrollierbarer Einsatz wäre. Das ist ein Thema, das sich auch beim Fiff durch die letzten Jahrzehnte zieht.

Umweltschädigung überwachen

Constanze Kurz: *Was brennt denn thematisch gerade unter den Nägeln? Und was könnte ein noch stärkeres Thema in Zukunft sein?*

Hans-Jörg Kreowski: Rainer hat noch nicht über Nachhaltigkeit und *Bits & Bäume* gesprochen. Die Klimakatastrophe ist absehbar, sie wird nicht vermieden werden, sondern nur gedämpft. Daher ist die Mitarbeit des Fiff in der Initiative *Bits & Bäume* eine ganz wichtige Sache. In diese Richtung wird das Fiff ganz viel in Zukunft machen müssen.

Insbesondere denke ich auch, dass man Informationstechnik ohne Weiteres nutzen können müsste zur Überwachung, Kontrolle und Planung von Maßnahmen, die den Klimawandel dämpfen. Wettervorhersage funktioniert schon erstaunlich gut. Warum soll Umweltschädigung nicht genauso gut überwacht werden können? Die Militärs glauben ja auch, dass sie die ganze Welt bis zum kleinsten Panzer, der irgendwo umherfährt, beobachten können. Also müssten wir eigentlich dieselbe Technik nutzen können, um etwas für die Umwelt zu tun.

Was auf jeden Fall bleibt als Thema: Rüstung und Informatik. Wir haben ja seit fast zehn Jahren die Cyberpeace-Kampagne. Sie muss wahrscheinlich ein bisschen modernisiert und aufgefrischt werden, aber das ist ein Thema, von dem wir nicht loskommen.

Rainer Rehak: Ich würde gern noch einiges anfügen. Ganz konkrete Themen sind auch der digitale Produktpass oder das Lieferkettengesetz: Wo kommt eigentlich die Technik her? Wer schraubt die zusammen, wo kommen die Materialien her? Von Kinderarbeit bis zu neuen Arbeitsnormen, das findet aktuell auf EU-Ebene statt, auch das Recht auf Reparatur, der Akkuaustausch und gleiche Anschlüsse für Ladegeräte.

In der Diskussion um Nachhaltigkeit beschäftigen uns auch die Zertifikate Blauer Engel für Software und Blauer Engel für Hardware. Man muss natürlich diskutieren, wie gut oder schlecht solche Siegel sind. Der nächste Schritt ist dann, dafür zu sorgen, dass es diese Standards auch für öffentliche Stellen geben sollte. Da gibt es ganz konkrete Vorhaben, wo wir uns einklinken.

Gerade gab es eine Diskussion auf EU-Ebene über automatisierte Gesichtserkennung auf öffentlichen Plätzen. Auch soll es bald für die Datenschutzgrundverordnung vielleicht ein Update geben. Diese Diskussionen sind sehr wichtig, wenn es darum geht, was wir gelernt haben aus den letzten sechs bis acht Jahren Datenschutzgrundverordnung. Was hat funktioniert, was nicht?

Und natürlich beschäftigt uns auch der große Themenbereich IT-Sicherheit, vom staatlichen Hacking und den Entwicklungen beim BSI bis zu den Implikationen zur Cyber-Sicherheitsstrategie. Dass in der Cyber-Sicherheitsstrategie keine Sicherheit steckt, konnten wir zeigen⁷. Aber auch auf EU-Ebene stand die Entwicklung zu Mindeststandards für IT-Sicherheit an. Wir äußern wir uns sowohl mit Debattenbeiträgen als auch in Anhörungen⁸.

Meist ehrenamtliche Arbeit

hekta: *Das hört sich nach einer Menge Arbeit und nach vielen Themen an. Dazu braucht es viele Mitglieder. Auf der Webseite habe ich die Zahl 700 gelesen, stimmt das?*

Rainer Rehak: Es sind jetzt knapp 700 Mitglieder, Tendenz steigend. Man muss dazu sagen: Natürlich sind nicht alle Mitglieder aktiv, aber wir haben mittlerweile sechs Regionalgruppen, in denen auch Projekte gemacht werden: Konsultationen, Demos oder Vorträge. Teilweise sind es aber auch Cryptopartys, wo man sich einfach trifft und über die Sicherheit von Geräten spricht.

Die Arbeit liegt nicht auf 700 Schultern, aber doch auf einigen Schultern verteilt. Wer Interesse an unseren Themen findet, kann gern Mitglied werden oder einfach nur mitarbeiten, auch als Nichtmitglied. Das Schöne ist, dass wir durch die steigenden Mitgliederzahlen und auch durch Projektarbeiten mittlerweile drei Angestellte haben. Das heißt, wir sind gerade in dem Prozess der Professionalisierung, um unsere Themen noch besser voranzutreiben.

Constanze Kurz: *Wir haben das noch nicht erwähnt: Die Vereinsmitgliedschaft und die Engagierten betreiben eine Form von Aktivismus, das ist zumeist ehrenamtliche Arbeit. Wie viele Leute machten denn am Anfang mit? Wie war die Entwicklung, bis ihr jetzt zu diesen 700 Leuten gekommen seid?*

Hans-Jörg Kreowski: Angefangen hat die ganze Sache mit gut 200 Gründungsmitgliedern. Wir sind bis fast 1.000 hochgekommen. Dann ging es aber in den 2000-er Jahren langsam wieder runter.

Milliarden für „unbemenschte Waffen“

Constanze Kurz: *Ich würde gern konkret zum Militär und zu Rüstungsfragen kommen: Definitiv war der NATO-Doppelbeschluss einer der Gründungsimpulse, und ihr steht auch auf den Schultern der Friedensbewegung. Wie hat sich die Sicht auf die Zusammenarbeit von Informatiker:innen mit Militärs gewandelt? Wohin werden die großen Summen verteilt, über die wir nicht mehr reden? Wo würdet ihr euch heute verorten?*

Hans-Jörg Kreowski: Die Verstrickung von Informatik und Militär ist ein Hauptthema, weil das Militär ein Haupttreiber für die Informatik-Entwicklung war. Tatsächlich sind nun weitere treibende Kräfte dazugekommen. Das Militär ist weiterhin ganz nachdrücklich insbesondere mit Geld und Wünschen und Anforderungen an die Informatik herantreten.

Die ganze Welt rüstet für den Cyberkrieg auf und das heißt ja programmieren, programmieren, programmieren, etwa um beliebige technische Systeme zu infiltrieren, zu übernehmen und umzufunktionieren. Die NATO macht riesige Übungen jedes Jahr mit hunderten Teilnehmer:innen dazu. Da passiert unglaublich viel, von dem wir im Detail gar nicht viel wissen, sondern in der Zeitung nur über die militärischen Übungen lesen.

Dann kommt der große Bereich der unbemenschten Waffen dazu. Sie werden seit den 1980er-Jahren entwickelt. Waffensysteme sind natürlich oft unbemenschte. Aber hier geht es um Systeme, die wie Panzer, Boote oder Flugzeuge normalerweise

Besetzungen haben. Die Besetzung wird mehr und mehr herausgenommen. Dafür werden Milliarden pro Jahr ausgegeben.

Bei den USA weiß man das, sie haben das mal quantifiziert: jedes Jahr drei Milliarden US-Dollar. Wir in Europa werden wahrscheinlich noch mehr ausgeben und andere geben mindestens genauso viel aus. Das wurde in der Zwischenzeit unglaublich weit vorangetrieben, so dass die Systeme teils im Einsatz sind. Trotzdem wird das natürlich auch noch weiterentwickelt.

Der nächste Schritt aber, der sich jetzt unmittelbar abzeichnet, ist zum Beispiel bei der Entwicklung des *Future Combat Air System* von Frankreich, Deutschland und Spanien begonnen worden. Da soll bis 2040 ein neues Kampfflugzeug entwickelt werden, das dann in Drohnenschwärmen in der ganzen Welt Lufthoheit für Deutschland und Frankreich erzeugen soll. Das ist eine wahnwitzige Vorstellung, dass Deutschland und Frankreich die Lufthoheit haben sollen. Das kostet in der Entwicklung mindestens 100 Milliarden Euro, und die Anschaffung und der Betrieb nachher noch das Fünffache.

Das Geld ist im Moment gar nicht da. Insofern kann das auch noch scheitern. Aber was Informatik daran interessiert: Das ganze System soll von einer KI-Plattform aus geplant, gesteuert, organisiert werden. Das ist eine Art von KI-System, das es noch nicht gibt. Da wird wahrscheinlich unglaublich viel KI-Potenzial einfließen.

Es gibt auch beispielsweise Pläne vom Heeresamt der Bundeswehr, wie ein Krieg in einer Stadt aussieht, wie also Drohnen und Fahrzeuge autonom mit den Soldaten zusammen Krieg führen. Die Stadt ist dann aber so kaputt wie alle Städte, die in den Kriegen der letzten Jahrzehnte kaputt gemacht worden sind.

Das heißt: Der neue Krieg ist das alte Töten und Zerstören. Die eigentliche Aufgabe lautet: Damit muss Schluss sein.

Rainer Rehak: Es gibt militärisch natürlich viele Entwicklungen, die nicht so sichtbar in Waffenform stattfinden, sondern im Digitalen. Die Bundeswehr nennt es den Cyber- und Informationsraum⁹, wo sie sich stärken wollen: von offener Informationsbeschaffung über verdeckte Teilnahme an Kommunikation bis hin zu „aktiven Wirkmitteln“. Gemeint ist damit, die Offensivkapazitäten – das Hacking -auszubauen. Aber auch in der Art der Aufklärung selber tut sich da gerade sehr viel. Das Ziel, so nennt es die Bundeswehr, ist das gläserne Gefechtsfeld, wo quasi aus diversen Datenquellen eine Art Echtzeitlagebild inklusive der digitalen Geräte entstehen soll.

Momentan wird wieder über solche Fragen diskutiert, die gesellschaftliche Weichen stellen könnten: Wofür werden die Milliarden verwendet und setzen wir sie für Friedens- oder für Kriegsforschung ein?

Ein Beispiel sind die Zivilklauseln. Davon gibt es in Deutschland rund 70. Allerdings gibt es in Hessen und in Bayern Bestrebungen, die Zivilklauseln zu reduzieren oder teilweise sogar abzuschaffen. Dies sei im Sinne der Landesverteidigung und Sicherheitspolitik.

Die größten Erfolge stehen noch aus

hekta: *Wie erreicht euch Feedback?*

Rainer Rehak: Da wir ja beide in der Wissenschaft aktiv sind, haben wir auch mit politischen Akteuren zu tun. Man darf sich natürlich nicht der Illusion hingeben, dass fünf Leute ein Jahr lang an etwas arbeiten und dann ändert sich fundamental etwas an der Welt. Das sind alles sehr dicke Bretter, die wir bohren.

Wir bekommen aber immer wieder über individuelle Zuschriften oder nach Vorträgen mit, dass unsere Beiträge als Argumentationsgrundlage genutzt werden, beispielsweise in Ministerien oder von Leuten, die wissenschaftlich arbeiten.

Constanze Kurz: Was waren bisher die größten Erfolge des FfF? Wo habt ihr am meisten Wirkung entfaltet?

Hans-Jörg Kreowski: Die kontinuierliche Arbeit ist besonders wichtig. Wir bringen regelmäßig Publikationen heraus. Tatsächlich glaube ich, dass die größten Erfolge noch ausstehen. Ich würde mir zum Beispiel wünschen, dass sich mal ein paar Mäzene finden, die drei, vier Stellen auf Dauer finanzieren, damit wir dem bisschen Geld nicht permanent nachrennen müssen.

Die Technikentwicklung ist so gigantisch viel größer als die Technikfolgenabschätzung. Da wünsche ich mir viel mehr Fairness und vielleicht Zusammenarbeit, so dass man viele Dinge gleich von Anfang an vermeidet. Aber das sind alles Zukunftswünsche. Das hält mich aber beim FfF.

Constanze Kurz: Vielen Dank, dass ihr euch die Zeit für das Interview genommen habt!

Offenlegung: Zum Beirat des FfF¹⁰, der den Verein in wissenschaftlichen und satzungsmäßigen Angelegenheiten berät, gehört auch Constanze Kurz.

Quelle: <https://netzpolitik.org/2024/40-jahre-fff-gegen-die-unheilvolle-verflechtung-von-informatik-und-militaer-2/>

Anmerkungen

- 1 <https://blog.fiff.de/about/>
- 2 <https://snowflake.fiff.de/>
- 3 <https://blog.fiff.de/about/>
- 4 <https://blog.fiff.de/fiffkon2023-perspektiven-zukunftsvisionen-chancen-utopien/>
- 5 <https://www.fiff.de/verfaelschte-studie-zur-tauglichkeit-grundrechtswidriger-techniken.html>
- 6 <https://www.fiff.de/dsfa-corona>
- 7 <https://www.fiff.de/presse/Cybersicherheitsstrategie2021.html>
- 8 <https://www.fiff.de/presse/eIDmobilBiometrie.html>
- 9 <https://www.bundeswehr.de/de/organisation/cyber-und-informationsraum/kommando-und-organisation-cir/kommando-cyber-und-informationsraum>
- 10 <https://blog.fiff.de/beirat/>
- 11 https://de.wikipedia.org/wiki/Constanze_Kurz
- 12 <https://nowyouknow.eu/>
- 13 <http://gewissensbits.gi.de/constanze-kurz/>
- 14 <https://www.randomhouse.de/Buch/Cyberwar-Die-Gefahr-aus-dem-Netz/Constanze-Kurz/C.-Bertelsmann/e537921.rhd>
- 15 <http://www.faz.net/aktuell/feuilleton/aus-dem-maschinenraum/>
- 16 <https://www.youtube.com/watch?v=hj3gAsqrB18>
- 17 <http://www.ev-akademie-tutzing.de/toleranz-preis-fuer-christian-wulff-und-constanze-kurz/>
- 18 <mailto:constanze@netzpolitik.org>
- 19 <https://keys.openpgp.org/vks/v1/by-fingerprint/58ACBDA9D67D462D249605444A13B8EE269F8A45>
- 20 <https://blog.fiff.de/vorstand/>
- 21 <https://wissenschaft-und-frieden.de/>
- 22 <https://www.fiff.de/veranstaltungen/grundrechte-report2024.html>
- 23 <https://www.weizenbaum-institut.de/forschung/digitale-technologien-in-der-gesellschaft/digitalisierung-nachhaltigkeit-und-teilhabe/>
- 24 <https://bits-und-baeume.org/>



Die Gesprächsteilnehmer:innen

hekta war von April bis Juli 2024 Praktikantin bei netzpolitik.org. Sie beschäftigt sich mit Polizeigesetzen und Rechtsverschärfungen. Außerdem ist sie keine Freund:in von Unternehmen oder Institutionen, die immer die Identität von Menschen feststellen wollen, und würde gerne mehr über deren Methoden berichten. Darüber hinaus interessiert sie sich für den Schutz sensibler Daten auf Gesundheitsdatenbanken.

Constanze Kurz¹¹ ist promovierte Informatikerin, Autorin und Herausgeberin¹² von Büchern¹³, zuletzt *Cyberwar*¹⁴. Ihre Kolumne *Aus dem Maschinenraum*¹⁵ erschien von 2010 bis 2019 im Feuilleton der FAZ. Sie lebt in Berlin und ist ehrenamtlich Sprecherin¹⁶ des Chaos Computer Clubs. Sie war Sachverständige der Enquête-Kommission *Internet und digitale Gesellschaft* des Bundestags. Sie erhielt den Toleranz-Preis¹⁷ für Zivilcourage und die Theodor-Heuss-Medaille. **Kontakt:** E-Mail¹⁸ (OpenPGP¹⁹)

Hans-Jörg Kreowski ist Professor (i.R.) für Theoretische Informatik an der Universität Bremen. Er ist Mitglied im Vorstand des FfF²⁰ und Mitherausgeber der Zeitschrift *Wissenschaft und Frieden*²¹. Von 2019 bis 2022 war er außerdem Mitherausgeber des Grundrechte-Reports²². Inhaltlich beschäftigt er sich in Wort und Schrift vor allem mit der Verflechtung von Informatik und Rüstung sowie mit der Entlarvung der Technikmythen rund um Digitalisierung und Künstliche Intelligenz.

Rainer Rehak ist wissenschaftlicher Mitarbeiter in der Gruppe *Digitalisierung, Nachhaltigkeit und Teilhabe*²³ am Weizenbaum-Institut für die vernetzte Gesellschaft. Er promoviert an der TU Berlin zu systemischer IT-Sicherheit und gesellschaftlichem Datenschutz. Er studierte Informatik und Philosophie in Berlin und Hong Kong und beschäftigt sich seit über fünfzehn Jahren mit den Implikationen der Computerisierung der Gesellschaft. Er ist Ko-Vorsitz des FfF und Mitinitiator der *Bits & Bäume*-Konferenz für Digitalisierung und Nachhaltigkeit²⁴.

DATENSCHUTZ überall – außer in der *Praxis*?

Jörg Pohle, Stefan Hügel

Datenschutz überall – außer in der Praxis?¹

Editorial zum Schwerpunkt

Seit mehr als fünfzig Jahren gibt es spezielle Datenschutzgesetze, das Bundesdatenschutzgesetz ist 46 Jahre alt, die EG-Datenschutzrichtlinie fast 30 und die EU-Datenschutz-Grundverordnung auch schon wieder sechs Jahre. Die Diskussion um die unerwünschten Eigenschaften und Auswirkungen moderner Informatiksysteme und Informationsverarbeitungen ist sogar noch älter, und selbst die informatische Forschung zu möglichen Gegen- und Schutzmaßnahmen geht der rechtlichen Regulierung zeitlich voraus. Gerade vor diesem Hintergrund überrascht es umso mehr, dass wir ganz offensichtlich noch weit entfernt davon sind, datenschutzfreundliche Systeme in der Breite zu entwickeln und in die Praxis zu bringen.

Für dieses Scheitern bieten sich drei mögliche Erklärungen an. Erstens handelt es sich bei dem gesellschaftlichen Prozess, der weithin als *Digitalisierung* bezeichnet wird, um ein *bewegliches Ziel*, das sich immer weiter entwickelt und ändert und dabei immer neue Herausforderungen produziert, die adressiert werden wollen. Zweitens fehlt es in der Debatte an einem geteilten Verständnis zur Frage, welche Eigenschaften und Auswirkungen moderner Informatiksysteme und Informationsverarbeitungen nach welchen Kriterien und für wen unerwünscht sind und wie daher Abhilfemaßnahmen aussehen sollen. Und drittens werden die konkreten Gestaltungs- und Verarbeitungsvorgaben, die etwa in den einschlägigen Gesetzen enthalten sind, nicht nur vor dem Hintergrund unterschiedlicher Problem- und Zielvorstellungen interpretiert und umgesetzt (siehe die zweite Erklärung), sondern oft genug ohne jede Vorstellung vom größeren Zusammenhang oder den übergeordneten Zielen, denen sie dienen sollen.

Was hindert uns an wirksamem Datenschutz?

Mit den drei angesprochenen Gründen erheben wir nicht den Anspruch, das Fehlen von wirksamem Datenschutz in der Praxis abschließend oder widerspruchsfrei erklären zu können. Die angeführten Gründe überschneiden sich mindestens teilweise, und es gibt sicher weitere Gründe, darunter ökonomische. Nicht zuletzt geht es hier um Interessengegensätze: Organisationen gestalten und betreiben Informatiksysteme entsprechend ihren eigenen Interessen, während sie die Interessen von Beschäftigten, Nutzer:innen oder Betroffenen ignorieren oder übergehen – wer die Technik und ihren Einsatz kontrolliert, zieht daraus die Vorteile; die negativen Auswirkungen werden externalisiert. Vor diesem Hintergrund ist der Datenschutz um 1970 angetreten, „Vorkehrungen zur Verhinderung unerwünschter Folgen von Informationsverarbeitung“ zu treffen und in die Praxis zu bringen, wobei als unerwünscht jede Folge der Informationsverarbeitung

verstanden wurde, „die den Zielen unserer Gesellschaft zuwiderläuft oder sie wenigstens gefährdet“, die „vor allem niedergelegt [sind] im Grundgesetz der Bundesrepublik Deutschland; namentlich in den Grundentscheidungen dieser Verfassung, die sich bekennt zu einer rechts- und sozialstaatlich verfaßten, das Individuum und die gesellschaftlichen Gruppierungen (insbesondere Minderheiten) schützenden parlamentarischen Demokratie“ (Steinmüller et al. 1972: 44).

Seitdem hat sich viel geändert: Immer neue informationstechnische Artefakte haben die Welt überschwemmt, immer mehr Bereiche der Gesellschaft wurden „informatisiert“ (Nora & Minc 1979), vom persönlichen und familiären Umfeld bis zur Sphäre der bürgerlichen Öffentlichkeit, von der Wirtschaft über Politik, Verwaltung und Militär bis zu Bildung, Wissenschaft und Medien. Jeder Technikgeneration wurden alle möglichen Wunderwirkungen zugeschrieben, ebenso alle möglichen Risiken (Pohle & Lenk 2021). So Phänomen- und Hype-getrieben wie die öffentliche Debatte war und ist, zeigte und zeigt sich auch die politische. Das hat zu einem gesetzgeberischen Flickenteppich geführt, der immer gleiche Probleme immer wieder neu, mit jeweils anderen Anwendungskriterien, den gleichen oder allenfalls leicht veränderten Zielvorstellungen, aber oft anderer Terminologie und mehr oder weniger neuen Einzelregelungen adressiert. Ein Beispiel dafür ist das Verhältnis zwischen der EU-Datenschutz-Grundverordnung und der EU-Verordnung über künstliche Intelligenz.

Die EU-Datenschutz-Grundverordnung geht von der Annahme aus, dass bei der Verarbeitung personenbezogener Daten Risiken für Menschen und ihre Grundrechte und -freiheiten erzeugt werden, und zielt daher darauf ab, die Menschen und ihre Grundrechte zu schützen (Artikel 1 Absatz 1 & 2 DSGVO). Dass Grundrechte und -freiheiten auch bei anderen Informationsverarbeitungen Risiken ausgesetzt sind, die adressiert – verhindert, minimiert oder kompensiert – werden müssen, sollte auch den extremsten Anhänger:innen der DSGVO spätestens dann deutlich geworden sein, als der europäische Gesetzgeber mit der KI-Verordnung ein Regelwerk auf den Weg gebracht hat, das das gleiche Ziel verfolgt – den Schutz der Grundrechte und -freiheiten, nur eben vor den „schädlichen Auswirkungen von KI-Systemen“ (Artikel 1 Absatz 1 KI-Verordnung). Beide Regelwerke sind konsequentialistisch² und zielen auf die gleichen unerwünschten Auswirkungen von modernen Informatiksystemen, haben aber voneinander unabhängige Anwendungskriterien (*personenbezogener Daten* vs. *KI-Systeme*) – und beide teilen die gleichen Schattenseiten: Es scheint für den Gesetzgeber komplett akzeptabel zu sein, wenn Risiken für Grundrechte und -freiheiten erzeugt und auf Betroffene abgeladen werden, solange das nur

eben mit Informatiksystemen und darauf ablaufenden Informationsverarbeitungen geschieht, die nicht mit *personenbezogenen Daten* operieren oder als *KI-Systeme* zählen. Naja, jedenfalls bis zum nächsten Hype und zum nächsten gesetzgeberischen Aktivismus – dann trifft es vielleicht User-Interfaces, Blockchains – der Gesetzgeber ist ja immer auch ein bisschen langsam –, „blaue Daten“ oder Informatiksysteme „an Donnerstagen“ ...

Eine mögliche Erklärung dafür, warum wir weit entfernt davon sind, datenschutz-, d. h. grundrechts- und freiheitsfreundliche Systeme in der Breite zu entwickeln und in die Praxis zu bringen, liegt in diesem Phänomen- und Hype-getriebenen Vorgehen und dem darauf aufbauenden gesetzgeberischen Aktivismus, die das Rad immer wieder neu erfinden, jede neue Version des Rades in Gesetzesform gießen und dabei jeweils andere Umsetzungsvorgaben machen, die auf willkürliche Art und Weise inkompatibel mit den Vorgaben sind, die für die vorherigen Versionen des Rades formuliert wurden.

Wenn es bisher in diesem Editorial so scheinen konnte, als herrsche Einigkeit darüber, welche Auswirkungen von Informatiksystemen wie verstanden und adressiert werden müssen, die Gegenmaßnahmen seien aber bisher nur unreflektiert und willkürlich in Gesetze gegossen worden, ist das bei näherem Hinsehen keineswegs so. Ganz im Gegenteil: Es gibt eine Unzahl von miteinander konkurrierenden und einander widersprechenden Vorstellungen über das, was als Probleme zu verstehen sei, was dafür aufseiten der Informatiksysteme, der Informationsverarbeitung und der beteiligten Akteure jeweils Ursachen oder Auslöser sein solle, und wie und von wem diesen Problemen abgeholfen werden müsse. Kurz: auf welche Ziele hin die Systeme und ihr Einsatz gestaltet und umgesetzt sein sollen. Das Problem ist nicht allein ein terminologisches, auch wenn es vielleicht im Hinblick auf die Terminologien am deutlichsten zutage tritt. Da streiten sich die Beteiligten darum, ob es um *Surveillance*, *Privacy* (oder *Privatheit* oder *Privatsphäre*) oder *Datenschutz* geht – und dem Ganzen ist dann noch eine ganz eigene, nämlich rechtliche Sicht übergestülpt, die mit ihrer eigenen Terminologie daherkommt, aber eben auch ihren eigenen Vorstellungen und Grenzziehungen. Und die Folgen dieser unterschiedlichen Sichtweisen zeigen sich dann darin, mit welchen Zielen und nach welchen Kriterien Informatiksysteme gestaltet und eingesetzt werden, welche unerwünschten Auswirkungen adressiert werden und welche nicht (Pohle 2019).

Ein paar Beispiele für die Gegensätze sollen genügen: Aus Sicht des geltenden *Datenschutzrechts* stellt eine erfolgreiche Anonymisierung eine *Lösung* dar, weil der Anwendungsbereich der Datenschutzgesetze beschränkt ist auf die Verarbeitung *personenbezogener Daten* und dieser damit verlassen wird. Aus Sicht des Datenschutzes kann das nicht ausreichen, denn: Relevant ist dort einzig, ob damit die unerwünschten Auswirkungen – für Individuen, Gruppen, Organisationen und die Gesellschaft, für Grundrechte und andere gesellschaftliche Werte und Ziele – verhindert werden oder nicht (vgl. Pohle & Hölzel 2020). *Privacy Impact Assessments* und *Privacy by Design* mögen Privatsphäre- oder Privatheitsprobleme identifizieren und lösen können, aber wie die Erfahrungen in der praktischen Umsetzung zeigen, werden dabei von den Beteiligten andere Grundrechte und die dafür entstehenden Risiken schlicht ignoriert. So können sie am Ende eben auch nicht adressiert werden (vgl. Frie-

dewald et al. 2022). Oder die Trinität von individueller Information, Einwilligung und Datenkontrolle – verbreitet in Framings wie *Empowerment*, *digitaler Souveränität* oder *Datensouveränität* –, die allenfalls eine operative Umsetzung ist, wird als das eigentliche Ziel verstanden. Die Frage von Auswirkungen der Informatiksysteme und ihres Einsatzes, ob auf individuelle oder kollektive Grundrechte oder andere gesellschaftliche Werte, ob erwünscht oder unerwünscht, stellt sich dann erst gar nicht – und sie kann in dieser Verständniswelt auch gar nicht gestellt werden (vgl. Pohle 2022).

Und nicht zuletzt liegt eine mögliche Erklärung dafür, warum wir noch weit entfernt davon sind, datenschutzfreundliche Systeme in der Breite zu entwickeln und in die Praxis zu bringen, in der Fixierung auf konkrete Operationalisierungen von Anforderungen in Einzelregelungen innerhalb von Gesetzen. Sie sollen dann unabhängig von ihrem Kontext und den übergeordneten Zielen umgesetzt werden, denen sie dienen sollen. Die meisten Leser:innen werden diesem Problem in der Praxis schon begegnet sein: Menschen, die glauben, dass es ausreicht, in den Gesetzen eine passende Rechtsgrundlage für die Verarbeitung zu finden (wie viele Jurist:innen), IT-Sicherheitsmaßnahmen auf dem Stand der Technik umzusetzen (wie viele Informatiker:innen) oder alles im von der DSGVO geforderten Verzeichnis der Verarbeitungstätigkeiten zu dokumentieren (wie viele Praktiker:innen). Nicht jede mögliche Schutzmaßnahme, auch nicht jede, die explizit im Gesetz aufgeführt ist, schützt jedes Grundrecht in jedem Kontext vor jedem Risiko. Nur ein paar Beispiele zu den Grundsätzen für die Datenverarbeitung (Artikel 5 Absatz 1 DSGVO): Transparenz schützt nicht vor Zensur, Vertraulichkeit nicht vor Diskriminierung, Richtigkeit nicht vor Stigmatisierung, und Datenminimierung kann die zukünftige Gesundheit beeinträchtigen, weil niemand heute weiß, ob und wann die Daten jemals erforderlich werden können.

Die Beiträge im Heftschwerpunkt

Die im Heftschwerpunkt versammelten Beiträge beleuchten unterschiedliche Aspekte im Bereich der datenschutzfreundlichen Gestaltung und Entwicklung von Informatiksystemen und deren Einsatz in der Praxis. Alle drei Beiträge adressieren einige der im Editorial aufgeworfenen Probleme, mit jeweils anderen Schwerpunkten und in unterschiedlichen Flughöhen.

Der Beitrag *Implementing GDPR: A Perspective from Developers* von Yuwen Zhang, Frank Ebbers und Nicholas Martin untersucht die Veränderungen in der Umsetzung von *Privacy by Design* aus Sicht von Entwickler:innen und anderen Menschen, die direkt in die Entwicklung von Informatiksystemen eingebunden sind, seit dem Inkrafttreten der DSGVO vor sechs Jahren. Die Studie basiert auf den Ergebnissen von teilstrukturierten Interviews mit Expert:innen, die mit einer Literaturstudie unterfüttert sind. Substanzielle Änderungen wurden nicht beobachtet, aber etwas mehr Vorsicht oder Sorgfalt aufseiten der Unternehmen, wenn es um die Einhaltung datenschutzrechtlicher Vorgaben geht, vor allem aber eine Zunahme an bürokratischem Aufwand. Vielleicht ist es der englischen Sprache des Beitrags geschuldet, in der auch die internationale Debatte, gerade in der Informatik, geführt wird, und der dort häufig anzutreffenden *Sprachverwirrung*. Es ist doch beachtenswert, dass erstens überall von *Privacy*

by Design die Rede ist, nicht aber von *Data Protection by Design*, wie es in der englischsprachigen Fassung der DSGVO heißt (der *General Data Protection Regulation, GDPR*), und zweitens an keiner Stelle über Grundrechte gesprochen wird – oder über die Grundrechtsrisiken. Nach der DSGVO sollen doch diese Grundrechtsrisiken „zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung [d. h. der Gestaltung und Umsetzung] als auch zum Zeitpunkt der eigentlichen Verarbeitung“ durch „geeignete technische und organisatorische Maßnahmen“ adressiert werden, „um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen“ (Artikel 25 Absatz 1 – *Datenschutz durch Technikgestaltung* bzw. im Englischen *Data Protection by Design*).

Artikel 25 Absatz 1 verlangt explizit die Berücksichtigung der „Risiken für die Rechte und Freiheiten natürlicher Personen“, bietet dazu allerdings kein besonderes Verfahren oder keine geeignete Methode an. Wenn hingegen die Verarbeitung „voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge“ hat oder haben kann, dann muss vorab eine explizite Datenschutz-Folgenabschätzung durchgeführt werden (Artikel 35 Absatz 1). Vor diesem Hintergrund kann das, was in Artikel 25 gefordert wird, auch als *kleine* (oder informelle) Datenschutz-Folgenabschätzung verstanden werden.

Der Beitrag *Durchführung einer Datenschutzfolgenabschätzung nach SDM* von Karin de Lange führt in die Thematik ein und stellt dazu den Ansatz des Standard-Datenschutzmodells (SDM) vor. Mit dem SDM lassen sich in strukturierter Weise die Identifikation und Bewertung von Risiken, die aus der Verarbeitung folgen können, und deren „Lösung“, d. h. Verhinderung, Minimierung oder Kompensation, durchführen. Zugleich erlaubt ein solches Vorgehen eine (vergleichsweise) einfache Erfüllung der in Artikel 5 Absatz 2 und Artikel 25 Absatz 1 DSGVO kodifizierten Rechenschafts- und Nachweispflichten.

Mit der Verwendung des Standard-Datenschutzmodells lässt sich zugleich eines der Probleme angehen, die die Umsetzung der datenschutzrechtlichen Anforderungen in der Praxis – auch in der Software-Entwicklungspraxis – prägen: die verbreitete Verwendung von Checklisten und anderen echten oder vermeintlichen *einfachen* Ansätzen oder vorgefertigten *Lösungen* – und, wie Entwickler:innen im Beitrag *Implementing GDPR* zitiert werden, der Forderung nach „mehr davon“. Der Beitrag *Warum Checklisten im Datenschutz kaum noch sinnvoll sind. Besser: „einfach.SDM.machen“* von Thomas Werning zeigt nicht nur

die Unzulänglichkeiten von Checklisten auf, sondern stellt ihnen auch zum Vergleich die Möglichkeiten gegenüber, die das Standard-Datenschutzmodell und seine Verwendung bieten.

Wir danken den Autor:innen ganz herzlich für ihre instruktiven Beiträge, den anonymen Reviewer:innen für ihre sehr kritischen und sehr konstruktiven Reviews und der Redaktion für die Möglichkeit, diesen Schwerpunkt zu gestalten.

Literatur

- Friedewald, M.; Schiering, I.; Martin N. & Hallinan, D. (2022), *Data Protection Impact Assessments in Practice. Experiences from Case Studies*. In: Katsikas, S. Et al. (Hg.), *Computer Security. ESORICS 2021 International Workshops*. Cham: Springer International Publishing, S. 424–443.
- Nora, S. & Minc, A. (1979), *Die Informatisierung der Gesellschaft*. Frankfurt am Main: Campus Verlag.
- Pohle, J. (2019), *Privacy and Data Protection by Design: A Critical Perspective*. In: Milch, R. S.; Benthall, S. & Potcovaru, A. (Hg.), *Building Common Approaches for Cybersecurity and Privacy in a Globalized World*, New York University, Center for Cybersecurity, S. 134–141.
- Pohle, J. (2022), *Datenschutz: Rechtsstaatsmodell oder neoliberale Responsibilisierung? Warum Datentreuhänder kein Mittel zum Schutz der Grundrechte sind*. In: Verbraucherzentrale NRW e.V. (Hg.), *Zu treuen Händen? Verbraucherdatenschutz und digitale Selbstbestimmung*.
- Pohle, J. & Hölzel, J. (2020), *Anonymisierung aus Sicht des Datenschutzes und des Datenschutzrechts. Stellungnahme zum Konsultationsverfahren des BfDI zur „Anonymisierung unter der DSGVO unter besonderer Berücksichtigung der TK-Branche“*.
- Pohle, J. & Lenk, K. (Hg.) (2021), *Der Weg in die „Digitalisierung“ der Gesellschaft – Was können wir aus der Geschichte der Informatik lernen?* Marburg: Metropolis-Verlag.
- Steinmüller, W.; Lutterbeck, B.; Mallmann, C.; Harbort, U.; Kolb, G. & Schneider, J. (1972), *Grundfragen des Datenschutzes. Gutachten im Auftrag des Bundesministeriums des Innern, BT-Drs. VI/3826, Anlage 1*.

Anmerkung

- 1 *Der Titel lehnt sich an das bekannte Bonmot von Robert Solow und Erik Brynjolfsson in dessen 1993er-Artikel „The Productivity Paradox of IT“ an: „computers are everywhere except in the productivity statistics“.*
- 2 *Konsequentialismus betrachtet die positiven und/oder negativen Folgen einer Sache oder Handlung, nicht die Eigenschaften der Handelnden (wie Tugenden, Gesinnungen, Ziele) oder der Sache oder Handlung selbst (wie Regeln, Prozesse, Pflichten bzw. deren Einhaltung).*



Jörg Pohle und Stefan Hügel

Dr. **Jörg Pohle** ist PostDoc am *Alexander von Humboldt Institut für Internet und Gesellschaft* (HIIG) in Berlin, wo er das Forschungsprogramm *Daten, Akteure, Infrastrukturen* co-leitet und sich unter anderem mit gesellschaftlichen Aushandlungen im Bereich Datenschutz und IT-Sicherheit 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.

Stefan Hügel ist seit 1993 Mitglied des FlfF, seit 1994 Diplom-Informatiker und seit 2009 FlfF-Vorsitzender. Er lebt und arbeitet in Frankfurt am Main.

Implementing GDPR: A Perspective from Developers

This study examines the changes in the implementation of Privacy by Design in software products from developers' perspectives six years after the enforcement of the General Data Protection Regulation (GDPR). Through semi-structured interviews with nine experts from seven different companies, we found that while the volume of data collected has not decreased, organizations have become more cautious. This increased caution is driven not only by stringent regulations but also by market and user demands. The study highlights the nuanced impact of the GDPR on data collection practices and the evolving role of developers in ensuring compliance and data protection.

Introduction

The General Data Protection Regulation (GDPR), which came into force in May 2018, is considered as the most impactful regulation in Europe and affects companies and consumers in multiple ways (De Chaves and Barreto Vavassori Benitti, 2023). To address the principle of Privacy by Design (PbD), one of the key issues of the GDPR, Article 25 and Recital 78 introduce the concept and practices of "Data Protection by Design". They mandate stringent levels of data protection, transparent data practices (Cavoukian, 2011), data minimization, effective control mechanisms for consumers and user friendliness (Working Party on Police and Justice, 2009).

There are several studies about the impact of the GDPR and the concept of PbD on companies and consumers (e. g. Almeida Teixeira et al., 2019; Hirvonen, 2022; Leite et al., 2022). For example, Freitas and Mira Da Silva (2018) identify the GDPR as too complex and thus challenging especially for small and medium enterprises (SMEs). Almeida Teixeira et al. (2019) highlight increased costs, human resources and additional administrative work. A survey of Norwegian companies found that 29 % of them find PbD a challenge for their business (Prethuis et al., 2018). Other authors have pointed "to a positive influence of privacy laws [...] on practitioners' behaviours and organizations' cultures" (Iwaya et al., 2023). However, an "analysis of [the GDPR's] impact on software engineering practices is an unexplored area" (Leite et al., 2022). This nonetheless, is important, as "the basis of implementation shifts away from traditional regulatory and legal professionals and towards privacy engineers" (Rommetsveit and Van Dijk, 2022) and privacy must be a priority of "engineers, computer programmers, and other technologists" (Waldman, 2018). Additionally, the need for PbD in software engineering (SE) becomes even more important. The number of apps that process and store highly personal and health data, e. g., for Covid-19 controlling in the past years, is increasing (De Chaves and Barreto Vavassori Benitti, 2023).

Further there are several calls by authors to investigate the role of engineers in PbD (e. g. De Chaves and Barreto Vavassori Benitti, 2023; Leite et al., 2022; Waldman, 2018). To address these calls and fill this research gap, we propose the following research questions: What changes have occurred from the perspective of engineers following the implementation of GDPR (RQ1)? How have product and design processes been affected (RQ2)? The remainder of this paper is structured as follows. First, we explain our methodology in detail. Next, the theoretical background examines the application of PbD and engineers' reactions to it, followed by a presentation of the empirical findings from our inter-

views. Finally, we discuss the implications of these findings and conclude this work with an outlook in the last chapter.

Methodology

Our methodology is two-fold. First, we conducted a literature review on the impact of PbD on engineers. Second, we used these findings and open questions to formulate interview questions and conducted the final interviews.

Literature review

We searched the ACM Basket of Eight and IEEE Xplore for overview knowledge. Then we conducted precise searches using Scopus and Google Scholar in October and November 2023. We used the following search term:

("Impact" OR "change" OR "Veränderung" OR "veränder" OR "Einfluss") AND („privacy by design" OR „privacy by default" OR „Article 25") AND (developer OR engineer OR designer OR Entwickler OR Programmierer) AND („GDPR" OR "DSGVO" OR "DS-GVO"),

followed by forward- and backward searches of selected papers. This resulted in a lot of papers from legal scholars, which we excluded.

Development of interview guideline and conducting interview

We used interviews because they can reveal information that is not available in literature nor through observation (Freitas and Mira Da Silva, 2018; Iwaya et al., 2023). Prior works, e. g., Waldman (2018) and Spiekermann et al. (2019) have already used interviews to gain insights into the engineers' perspective on privacy. Our goal was twofold: First, examine which behaviors found in the literature review have changed following the implementation of the GDPR and second, what other changes the GDPR had implied.

Our interview guideline contained demographical and company-related questions first, followed by four question blocks about: 1) mode of operation, 2) dealing with data protection in product development, 3) user centered design and 4) technology/product design processes. For a comprehensibility test, we consulted two experts and conducted a pre-test. Between De-

ember 2023 and mid-2024, we conducted semi-structured virtual interviews with nine male participants from diverse industries, all with backgrounds in programming or data protection. Participants were recruited through LinkedIn searches, emails, personal referrals, and the convenience sampling method. Initial screening ensured participants met the criteria outlined in the recruitment information. Seven individuals expressed interest, and two invited colleagues to join. All interviews were recorded with participants' consent, and audio was transcribed using an automated tool, followed by manual correction. Each participant was assigned an ID. Given that the GDPR has been in effect since 2018, analyzing the current employers of participants is less meaningful, as the interviews also addressed their prior work experiences.

Literature Review

Few papers have been written about changes in engineer's responses to privacy pre/post GDPR. Instead, prior work was written from a theoretical researchers' perspective (e.g., De Chaves and Barreto Vavassori Benitti, 2023), surveyed other regulations (Dias Canedo et al., 2020), focused on user experience in the user interfaces (Almeida and Monteiro, 2021), on specific GDPR articles (e.g., Art. 15 and 20 in Sørnum and Presthus, 2020) or on specific industries (e.g., Poritskiy et al., 2019). Papers that do concern the engineers' perspective, often come up with contradictory findings. For example Bednar et al. (2019) found "that systems engineers' concern for the privacy protection has grown over the past few years". In contrast, Benbenisty et al. (2021) found that developers often feel not responsible for privacy and "believe that they do not have the autonomy, the time, and the knowledge to incorporate privacy mechanisms".

Engineers' Reactions towards PbD

In a large-scale interview study with 80 participants, Waldman (2018) found that team lead engineers often viewed privacy as merely "giving users notice about their data". Spiekermann et al. (2019) surveyed 124 engineers and reported that 36 % rarely or never implement privacy mechanisms. Bednar et al. (2019) compared studies from 2003 and 2018, finding that engineers often address privacy only due to regulatory requirements, lacking a sense of responsibility, autonomy, and motivation. This aligns with findings from Hadar et al. (2018), Benbenisty et al. (2021). Benbenisty et al. (2021) and Spiekermann et al. (2019), who noted that developers often do not feel responsible for PbD or lack the expertise and time to implement it.

However, research lacks consideration of the perspective of engineers "who directly impact privacy implementation in software design" (Mazeli, 2022). There is limited research on privacy requirements compared to tools for detecting privacy leaks (e.g. Ebrahimi et al., 2019), leading to underperformance in privacy engineering across the software industry (Benbenisty et al., 2021). Engineers need to fully understand privacy concerns and be knowledgeable about privacy laws and standards (Iwaya et al. 2023, p. 4325). Additionally, research on the link between PbD implementation and engineers' individual factors remains inconclusive (Bu et al., 2020). Peixoto et al. (2023) found that

developers often focus on technical measures, doubt the effectiveness of privacy laws, lack time and autonomy, and misunderstand user privacy expectations.

PbD is "intended to bridge regulations with technical implementations" (Tahaei et al., 2021). However, engineers criticize this approach and mention downsides (De Chaves and Barreto Vavassori Benitti, 2023). Tamò-Larrioux (2018) criticizes the "loose definition" and highlights the need to break the principles "down into more concrete strategies". This has led to a situation, where "privacy decisions were made on the fly by engineers" (Waldman, 2018). This goes along with the challenge for engineers that the GDPR is technology-neutral (Almeida Teixeira et al., 2019). Colesky et al. (2016) suggest different privacy "tactics" for engineers "to make 'privacy by design' more practical". Furthermore, Aljeraisy et al. (2022) mention that the PbD principles "are rather disconnected from the real-life practice of systems engineering". In a structured literature review Saltarella et al. (2023) identifies several recommendations to engineers on how to apply PbD principals into practice. Furthermore, Bu et al. (2021) emphasizes the "practical problem of promoting PbD implementation through reasonable organizational measures". Iwaya et al. (2023) interviewed 30 engineers from non-European countries and found that only four actively used PbD approaches in their organizations.

Changes in addressing PbD by engineers post-GDPR

Whereas there is a stream of research about how engineers engage with PbD, research about the changes in this engagement after the enforcement of the GDPR is scarce. This is, despite published guidelines by data protection authorities on how to change in the software development life cycle (Datatilsynet, 2018) or examples of possible implementations (CNIL, 2022).

Some studies show that engineers struggle to understand the GDPR (De Chaves and Barreto Vavassori Benitti, 2023; Rommetveit and Van Dijk, 2022), especially without a legal background (Sirur et al., 2018). De Chaves and Barreto Vavassori Benitti (2023) found that post-GDPR, software engineering literature relies on Cavoukian's (2011) definition of PbD rather than providing new definitions. Leite et al. (2022) conducted case studies in Portuguese companies and found significant changes in "identifying requirements and modeling processes", as well as challenges in "adopting open standards and creating user-friendly designs", and issues with data erasure, auditing, and breach notifications. Dias Canedo et al. (2020) found that, similar to the GDPR, Brazil's LGPD significantly impacts the Requirements and Development disciplines. Agile teams face difficulties due to outdated requirements and limited stakeholder understanding of data privacy (Canedo et al., 2021). However, precise studies focusing on GDPR-induced changes from engineers' perspectives remain scarce.

Interview

In total, we conducted 7 interviews (P2 and P3, as well as P6 and P7, work at the same organization). Our interviewees were all male and had more than 5 years of job experience on aver-

age. This is in line with Balebako et al. (2014) who confirm most engineers to be male. The interviews lasted 40 minutes on average, were conducted online and recorded for transcription. Participants had the option to refuse audio recording.

ID	Gender	Experience [in years]	Position	Industry
1	M	15	Project leader	Mobility
2	M	5	Architect	Home appliances
3	M	10	Architect	
4	M	12	Full Stack Developer	Automotive
5	M	7	Data Protection Coordinator (DPC)	Retail industry (former) Automotive (current)
6	M	18	Chief Technology Officer	B2B SaaS (former)
7	M	13	Senior Engineering Manager	New Media
8	M	7	Consultant	Construction (former) Consulting (current)
9	M	5	Developer	Mobility

Table: Demographics of interviewees (Source: own illustration)

Summary of Interview Findings

Below we outline the topics that emerged from our interviews and discuss the changes our interviewees have experienced in their work since the GDPR was introduced in 2016. The key topics include agility, data collection, motivation and changes in work, and user interactions. The concept of PbD was prevalent across all four topics.

(a) Agility

Our interviewees unanimously agreed that agile practices make it easier to practically implement data protection. P2 and P3 indicated that data protection requirements, like other non-functional requirements, must adhere to specific regulations and guidelines. Agile development also offers a certain degree of flexibility in meeting legal and data protection requirements. This view was supported by P6 and P7, who mentioned that flexibility allows them to respond to market changes, although it also requires more effort. Team members of P8 and P9 are still working individually but also recognize the need to gradually transition to agile development.

(b) Data Collection

In the six years since the GDPR began to be enforced, the technologies to collect data have seen rapid advancement. This enables the collection of ever-greater amounts of data. P5 noted that “data is no longer just data; it is a crucial resource”, leading to increased data collection by companies. While P5 attributes this to both technological progress and the demand for data-driven operations, P4 emphasized the need for more data to improve service quality.

Companies are striving for a balance between enhancing services and ensuring data transparency and privacy. P1’s team is anonymizing data to comply with regulations, though P1 expressed a preference for collecting more data if the rules were less stringent – a sentiment shared by P9. Despite the growing volume of data, P5’s team remains committed to data minimization, using anonymization and pseudonymization to ensure compliance. P2 and P3, however, noted that the Federal Data Protection Act (BDSG) had already mandated data minimization before GDPR, so their practices haven’t changed significantly. In contrast, P6’s team only anonymizes or pseudonymizes data when it is highly sensitive.

(c) Procedural changes

Since the advent of GDPR, while the core nature of development work hasn’t fundamentally changed, engineers have had to allocate more time to data protection, leading to increased administrative processes, such as more detailed documentation, review, and approval procedures. P4 noted that GDPR has somewhat hindered development, as even small-scale research must adhere to strict procedures. P1, P2, and P3 mentioned that their teams spend significant time adjusting procedures when new regulations arise, with P2 and P3 viewing data protection as an added cost that doesn’t drastically alter work hours. P9 highlighted the need to integrate data protection from the project’s outset, requiring extensive collaboration with legal and administrative departments. P6 and P7’s teams have reallocated 20% of their staff to focus solely on GDPR compliance. Despite the two-year gap between GDPR adoption and enforcement, many companies only made necessary changes when required for business partnerships or to avoid penalties. As P1 summarized, “Punishment provides motivation”, noting that data breaches now carry severe legal and financial risks.

(d) Customer interaction

During interviews, P4 emphasized customer understanding and participation in data collection, aiming to show how data sharing benefits both individuals and society. P1 and P8 prioritize meeting legal requirements first, followed by customer preferences and procedural usability. In contrast, P2 and P3 prioritize fulfilling customer demands efficiently, aiming to minimize repeated consent requests. They noted that many users prefer minimal data usage and often do not read detailed data protection documents. P5 and P6 addressed challenges with consent management, implementing broader agreements and providing options for users to adjust preferences. Overall, while some users are privacy-sensitive, many willingly consent to data use, influenced by incentives and transparent data practices. P5 also mentioned the importance of data transparency. He stated that they must ensure data subjects (users) know which departments to contact to uphold their rights.

(e) PbD

“Privacy by Design is not only a legal requirement but also a market demand”, said P5. As a data protection officer, he needs to have a basic understanding of technology as well as a clear grasp of legal expertise. This allows him to communicate effectively and promptly with his programming colleagues. P1 mentioned that they incorporated PbD only after the implementation of GDPR and adjusted their approach whenever new partners joined. P2 and P3’s teams stated that they started implementing PbD during the product conceptualization and early development stages.

Discussion

The GDPR has become a significant source of concern for many organizations (De Chaves and Barreto Vavassori Benitti, 2023). The lack of enthusiasm for privacy mechanisms observed may stem from the perceived redundancy of these measures within established practices, a point also noted by Hadar et al. (2018). In addition to the findings from the study of Bednar et al. (2019), which highlighted engineers’ lack of autonomy, motivation, and sense of responsibility in addressing privacy-related issues, engineers also lack understanding and motivation to learn about GDPR (Alhazmi and Arachchilage, 2021), there was also a shortage of implementation technologies, tools, online resources (Danezis et al., 2014), and organizational support (Alhazmi and Arachchilage, 2021). Therefore, many companies did not immediately integrate PbD into their operations after the GDPR was enacted, a finding consistent with Iwaya et al.’s (2023) survey results. Today, PbD has become widespread, primarily driven by the threat of substantial fines. According to Article 83, companies can be fined up to 4 % of their global annual turnover or €20 million, whichever is higher, for serious breaches of data protection principles. This legal consequence is a major motivator for companies to adopt PbD.

However, as our interviews revealed, even under strict legal requirements, many companies assess the fines and costs before deciding on their actions. Another factor driving compliance is customer demand. To offer services to compliant companies and ensure their sustainability in an increasingly globalized world, organizations must adhere to the new regulations (Freitas and Mira Da Silva, 2018). In this study, we found that en-

gineers often perceive GDPR compliance as both a bureaucratic burden and a component of their development processes. This aligns with Spiekermann et al. (2019), while contrasting with the more integrated approach suggested by Iwaya et al. (2023). Additionally, managing data necessitates that organizations not only document existing data but also their processing activities (Lopes and Oliveira, 2018). This requirement undeniably increases costs and administrative burdens. Our findings underscore a significant gap in understanding the GDPR’s implications for software design, which aligns with concerns raised by Bu et al. (2020) about inconclusive research on PbD implementation.

Due to our limited sample size, our conclusions may be constrained. Guest et al. (2006) suggest that data saturation in qualitative studies typically occurs after about 12 interviews. Our study included seven interviews with nine participants, indicating a relatively small sample size. Additionally, some participants shared experiences from multiple companies, which may reduce the industry representativeness of our findings. Gill et al. (2008) note that effective semi-structured interviews generally range from 30 minutes to one hour. Ideally, in-depth interviews should last around one hour and can extend up to 90 minutes to thoroughly explore all questions and additional topics raised by interviewees. However, given the difficulty of recruiting what are often very busy people for interviews, we refrained from asking for more than 30-45 minutes of their time.

Conclusion

Our research confirms a growing emphasis on privacy among developers, a trend noted before the GDPR (Greene and Shilton, 2018). Companies adhering strictly to PbD principles during design and development can gain a competitive edge, as consumer privacy concerns rise. Increased transparency can enhance user trust in technology and organizations, boosting market competitiveness. However, this may increase the initial development cost and complexity. While GDPR has introduced substantial administrative processes for engineers, it has not fundamentally changed the nature of development work. Engineers are adapting by allocating more time to data protection and facing challenges related to data minimization and privacy integration. Our research highlights the need for better understanding and training regarding privacy regulations, as well as the importance of integrating privacy measures into the development lifecycle.

Yuwen Zhang, Frank Ebbers und Nicholas Martin

Yuwen Zhang graduated with a Master’s degree from the University of Göttingen and subsequently joined Fraunhofer ISI. Since November 2023, Yuwen has been working as a researcher. Their research focuses on information management and information security.

Frank Ebbers works as a corporate information security manager at ZEISS Group. He holds a Master’s degree in Business Informatics and a PhD in Information Systems. His doctoral thesis focused on human factors in information security in the Internet of Things era. From 2019 to 2023, he worked as a doctoral researcher at Fraunhofer ISI.

Nicholas Martin is a senior research scientist at Fraunhofer ISI. He holds a PhD in political science from MIT.

Overall, this study contributes to the ongoing discourse on privacy engineering and suggests that more comprehensive strategies are needed to align development practices with regulatory requirements. Future research should examine these strategies across different industries to provide a more detailed understanding of GDPR's impact on software engineering.

Acknowledgements

This work was funded by the German Ministry of Education and Research as part of the project PRIDS – [Privatheit, Demokratie und Selbstbestimmung im Zeitalter von Künstlicher Intelligenz und Globalisierung]

References

- Alhazmi, A., Arachchilage, N.A.G., 2021. I'm all ears! Listening to software developers on putting GDPR principles into software development practice. *Pers Ubiquit Comput* 25, 879–892. <https://doi.org/10.1007/s00779-021-01544-1>
- Aljeraisy, A., Barati, M., Rana, O., Perera, C., 2022. Privacy Laws and Privacy by Design Schemes for the Internet of Things: A Developer's Perspective. *ACM Comput. Surv.* 54, 1–38. <https://doi.org/10.1145/3450965>
- Almeida, F., Monteiro, J.A., 2021. Exploring the Effects of GDPR on the User Experience. *J INFORM SYSTEMS ENG* 6, em0140. <https://doi.org/10.21601/jisem/10957>
- Almeida Teixeira, G., Mira Da Silva, M., Pereira, R., 2019. The critical success factors of GDPR implementation: a systematic literature review. *DPRG* 21, 402–418. <https://doi.org/10.1108/DPRG-01-2019-0007>
- Balebako, R., Marsh, A., Lin, J., Hong, J., Faith Cranor, L., 2014. The Privacy and Security Behaviors of Smartphone App Developers, in: *Proceedings 2014 Workshop on Usable Security*. Presented at the Workshop on Usable Security, Internet Society, San Diego, CA. <https://doi.org/10.14722/usec.2014.23006>
- Bednar, K., Spiekermann, S., Langheinrich, M., 2019. Engineering Privacy by Design: Are engineers ready to live up to the challenge? *The Information Society* 35, 122–142. <https://doi.org/10.1080/01972243.2019.1583296>
- Benbenisty, Y., Hadar, I., Luria, G., Spoletini, P., 2021. Privacy as first-class requirements in software development: A socio-technical approach, in: *2021 36th IEEE/ACM International Conference on Automated Software Engineering (ASE)*. Presented at the 2021 36th IEEE/ACM International Conference on Automated Software Engineering (ASE), IEEE, Melbourne, Australia, pp. 1363–1367. <https://doi.org/10.1109/ASE51524.2021.9678872>
- Bu, F., Wang, N., Jiang, B., Jiang, Q., 2021. Motivating information system engineers' acceptance of Privacy by Design in China: An extended UTAUT model. *International Journal of Information Management* 60, 102358. <https://doi.org/10.1016/j.ijinfomgt.2021.102358>
- Bu, F., Wang, N., Jiang, B., Liang, H., 2020. "Privacy by Design" implementation: Information system engineers' perspective. *International Journal of Information Management* 53, 102124. <https://doi.org/10.1016/j.ijinfomgt.2020.102124>
- Canedo, E.D., Toffano Seidel Calazans, A., Cerqueira, A.J., Teixeira Costa, P.H., Seidel Masson, E.T., 2021. Agile Teams' Perception in Privacy Requirements Elicitation: LGPD's compliance in Brazil, in: *2021 IEEE 29th International Requirements Engineering Conference (RE)*. Presented at the 2021 IEEE 29th International Requirements Engineering Conference (RE), pp. 58–69. <https://doi.org/10.1109/RE51729.2021.00013>
- Cavoukian, A., 2011. *Privacy by Design in Law, Policy and Practice: A White Paper for Regulators, Decision-makers and Policy-makers*. CNIL, 2022. *Guide RGPD du développeur* [WWW Document]. URL <https://www.cnil.fr/fr/guide-rgpd-du-developpeur> (accessed 7.10.24).
- Colesky, M., Hoepman, J.-H., Hillen, C., 2016. A Critical Analysis of Privacy Design Strategies, in: *2016 IEEE Security and Privacy Workshops (SPW)*. Presented at the 2016 IEEE Security and Privacy Workshops (SPW), pp. 33–40. <https://doi.org/10.1109/SPW.2016.23>
- Danezis, G., Domingo-Ferrer, J., Hansen, M., Hoepman, J.-H., Le Métayer, D., Tirtea, R., Schiffner, S., 2014. Privacy and data protection by design: from policy to engineering. *European Union Agency for Network and Information Security (ENISA)*. <https://doi.org/10.2824/38623>
- Datatilsynet, 2018. *Innebygd personvern og personvern som standard* [WWW Document]. URL <https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/innebygd-personvern-og-personvern-som-standard/> (accessed 7.10.24).
- De Chaves, S.A., Barreto Vavassori Benitti, F., 2023. Privacy by Design in Software Engineering: An update of a Systematic Mapping Study, in: *Proceedings of the 38th ACM/SIGAPP Symposium on Applied Computing*. Presented at the SAC '23: 38th ACM/SIGAPP Symposium on Applied Computing, ACM, Tallinn Estonia, pp. 1362–1369. <https://doi.org/10.1145/3555776.3577626>
- Dias Canedo, E., Toffano Seidel Calazans, A., Toffano Seidel Masson, E., Teixeira Costa, P.H., Lima, F., 2020. Perceptions of ICT Practitioners Regarding Software Privacy. *Entropy (Basel)* 22, 429. <https://doi.org/10.3390/e22040429>
- Ebrahimi, F., Tushev, M., Mahmoud, A., 2019. Mobile App Privacy in Software Engineering Research: A Systematic Mapping Study. <https://doi.org/10.48550/arXiv.1910.03622>
- Freitas, M.D.C., Mira Da Silva, M., 2018. GDPR Compliance in SMEs: There is much to be done. *Journal of Information Systems Engineering & Management* 3. <https://doi.org/10.20897/jisem/3941>
- Gill, P., Stewart, K., Treasure, E., Chadwick, B., 2008. Methods of data collection in qualitative research: interviews and focus groups. *Br Dent J* 204, 291–295. <https://doi.org/10.1038/bdj.2008.192>
- Greene, D., Shilton, K., 2018. Platform privacies: Governance, collaboration, and the different meanings of "privacy" in iOS and Android development. *New Media & Society* 20, 1640–1657. <https://doi.org/10.1177/1461444817702397>
- Guest, G., Bunce, A., Johnson, L., 2006. How Many Interviews Are Enough?: An Experiment with Data Saturation and Variability. *Field Methods* 18, 59–82. <https://doi.org/10.1177/1525822X05279903>
- Hadar, I., Hasson, T., Ayalon, O., Toch, E., Birnhack, M., Sherman, S., Balissa, A., 2018. Privacy by designers: software developers' privacy mindset. *Empir Software Eng* 23, 259–289. <https://doi.org/10.1007/s10664-017-9517-1>
- Hirvonen, P., 2022. *A Review of GDPR Impacts on Information Security*. Iwaya, L.H., Babar, M.A., Rashid, A., 2023. Privacy Engineering in the Wild: Understanding the Practitioners' Mindset, Organizational Aspects, and Current Practices. *IEEE Trans. Software Eng.* 49, 4324–4348. <https://doi.org/10.1109/TSE.2023.3290237>
- Leite, L., Dos Santos, D.R., Almeida, F., 2022. The impact of general data protection regulation on software engineering practices. *ICS* 30, 79–96. <https://doi.org/10.1108/ICS-03-2020-0043>
- Lopes, I.M., Oliveira, P., 2018. Implementation of the general data protection regulation: A survey in health clinics, in: *2018 13th Iberian Conference on Information Systems and Technologies (CISTI)*. Presented at the 2018 13th Iberian Conference on Information Systems and Technologies (CISTI), pp. 1–6. <https://doi.org/10.23919/CISTI.2018.8399156>
- Mazeli, A., 2022. *A Framework to Support Software Developers in Implementing Privacy Features*. Peixoto, M., Ferreira, D., Cavalcanti, M., Silva, C., Vilela, J., Araújo, J., Gorschek, T., 2023. The perspective of Brazilian software developers on

- data privacy. *Journal of Systems and Software* 195, 111523. <https://doi.org/10.1016/j.jss.2022.111523>
- Poritskiy, N., Oliveira, F., Almeida, F., 2019. The benefits and challenges of general data protection regulation for the information technology sector. *Digital Policy, Regulation and Governance* 21, 510–524. <https://doi.org/10.1108/DPRG-05-2019-0039>
- Presthus, W., Sørnum, H., Andersen, L., 2018. GDPR COMPLIANCE IN NORWEGIAN COMPANIES.
- Rommetveit, K., Van Dijk, N., 2022. Privacy engineering and the techno-regulatory imaginary. *Soc Stud Sci* 52, 853–877. <https://doi.org/10.1177/03063127221119424>
- Saltarella, M., Desolda, G., Lanzilotti, R., Barletta, V., 2023. Translating Privacy Design Principles Into Human-Centered Software Lifecycle: A Literature Review. <https://doi.org/10.1080/10447318.2023.2219964>
- Sirur, S., Nurse, J.R.C., Webb, H., 2018. Are we there yet? Understanding the challenges faced in complying with the General Data Protection Regulation (GDPR).
- Sørnum, H., Presthus, W., 2020. Dude, where's my data? The GDPR in practice, from a consumer's point of view. *Information Technology & People* 34, 912–929. <https://doi.org/10.1108/ITP-08-2019-0433>
- Spiekermann, S., Korunovska, J., Langheinrich, M., 2019. Inside the Organization: Why Privacy and Security Engineering Is a Challenge for Engineers. *Proc. IEEE* 107, 600–615. <https://doi.org/10.1109/JPROC.2018.2866769>
- Tahaei, M., Frik, A., Vaniea, K., 2021. Privacy Champions in Software Teams: Understanding Their Motivations, Strategies, and Challenges, in: *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. Presented at the CHI '21: CHI Conference on Human Factors in Computing Systems, ACM, Yokohama Japan, pp. 1–15. <https://doi.org/10.1145/3411764.3445768>
- Tamò-Larrioux, A., 2018. *Designing for Privacy and its Legal Framework: Data Protection by Design and Default for the Internet of Things, Law, Governance and Technology Series*. Springer International Publishing, Cham. <https://doi.org/10.1007/978-3-319-98624-1>
- Waldman, A.E., 2018. DESIGNING WITHOUT PRIVACY. *HOUSTON LAW REVIEW*. Working Party on Police and Justice, 2009. *The Future of Privacy*.

Karin de Lange

Durchführung einer Datenschutzfolgenabschätzung nach SDM

Wer kennt nicht das Staunen und Interesse an prähistorischen Ausstellungsstücken bei Besuchen von Museen. Schon immer wurden Lebensarten und Risiken dokumentiert. Auch Schutzmaßnahmen gab es. Erinnern wir uns an Caesars Verschlüsselung. Es bestand das Risiko, dass Botschaften nicht unversehrt beim Empfänger ankommen, deshalb wurde diese Schutzmaßnahme ergriffen. Warum dann in der Gegenwart dieser Widerstand, Risiken durch Datenverarbeitung sehen zu wollen und Schutz zu gewährleisten. Das muss nicht sein.

Datenschutz

Der Begriff des Datenschutzes ist irreführend. Geschützt werden nicht die Daten, sondern die Rechte und Freiheiten von Menschen, über die Daten von deren Start ins Leben bis zum Ende verarbeitet werden. Auch das ist nicht neu. Schon immer wollten Menschen etwas über andere Menschen wissen. So haben sie entweder ihre Neugierde befriedigt oder Vorteile aus dem Wissen gezogen. Ein Schutzbedarf drängt sich auf.

Zur Verdeutlichung hier ein Beispiel:

Ein junger Mensch bat um Rat: „Zuhause flüstern wir uns nur noch die Passwörter zu.“ Eine Nachfrage ergab, dass es ein „Familienpasswort“ gibt und Amazons Sprachassistent Alexa aktiv ist. Das System soll nicht mithören. Experten empfehlen für jeden Nutzenden ein eigenes Passwort, damit u. a. auch Aktivitäten zugeordnet werden können (u. a. wer hat was wann und wo bestellt ...), und der Familie und Alexa täglich eine Pause zu gönnen.

Diese Expertenempfehlung ist eine erste Maßnahme. Eine Datenschutzfolgenabschätzung würde die nicht unmittelbar erkennbaren Risiken offenbaren, wie Überwachung der gesamten Lebensart (welche Musik, Bücher oder Filme, Termine, Sprache, Interessen etc.) durch das Unternehmen und Weitergabe der daraus generierten Informationen innerhalb des Unternehmens und an Dritte sowie Verhaltensanpassung (es wird geflüstert) und damit Steuerung der freien Entwicklung des Einzelnen mit erhöhtem Risikopotential für Kinder.

Intention des Datenschutzes ist es, unverhältnismäßige Eingriffe in die Rechte und Freiheiten von Menschen abzuwehren und schädliche Folgen der Verarbeitung personenbezogener Daten zu verhindern oder auf ein vertretbares Maß zu mildern.

Die Grundsätze für die Verarbeitung personenbezogener Daten legt Art. 5 DSGVO fest. Den besonderen Schutz von Kindern nimmt Erwägungsgrund 38 auf.¹

Was ist zu tun?

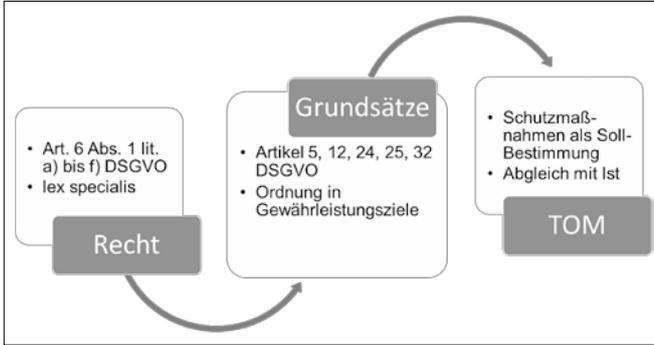
Der Gesetzgeber erlässt eine abstrakt-generelle Regelung. Sie ist verbindlich für eine unbestimmte Vielzahl von Fällen gegenüber einer unbestimmten Anzahl von Personen. Zur Umsetzung gibt es keine Vorgaben. Hier können Standards helfen. Der Duden bezeichnet den Standard als etwas, was als mustergültig, modellhaft angesehen wird und nach dem sich anderes richtet. Standards geben Halt und Sicherheit, wie z. B. Zeitzonen, Ampelfarben, Normen (wie ISO 27001) und der BSI-Grundsatz.

Die Standards ISO 27001 und BSI-Grundsatz werden von Unternehmen und anderen Organisationen – mit Ausnahme der Bundesbehörden – freiwillig verwendet. Sie sind etabliert und vertraut. Anders das Standard-Datenschutzmodell (SDM)². Seine Basis sind die in Artikel 5 Absatz 2 und Artikel 25 Absatz 1 DSGVO kodifizierten Rechenschafts- und Nachweispflichten. Die Konferenz der deutschen Aufsichtsbehörden für den Datenschutz (DSK) hat die Anwendung des SDM (zu-

letzt am 15.5.2024, SDM-V3.1, 107. DSK, TOP 10³) beschlossen, der IT-Planungsrat empfiehlt die Anwendung (Beschluss vom 25.3.2020⁴) und nach BSI-IT-Grundschutz-Kompendium CON.2, Edition 2023⁵, sollte die Nichtanwendung der SDM-Methodik begründet und dokumentiert werden.

Aktuell hat das Landgericht Mannheim in seiner Entscheidung am 15.3.2024⁶ das SDM zur Bewertung des Schutzniveaus auf eine Stufe mit dem BSI-Grundschutz gestellt.

Hier das SDM als Schaubild:



Es werden zunächst die rechtlichen Anforderungen erfasst. Sodann erfolgt eine Zuordnung zu den aus den wesentlichen Grundsätze des Art. 5 DSGVO abgeleiteten Gewährleistungszielen (siehe Tabelle oben rechts).

Anschließend erfolgt die Überführung in technische und organisatorische Schutzmaßnahmen, die sowohl als generische Maßnahmen als auch durch Bausteine vom SDM zur Verfügung gestellt werden.

DSGVO-Grundsätze Art. 5 Abs. 1	SDM-Gewährleistungsziele
a) „... müssen in einer für die Person nachvollziehbaren Weise verarbeitet werden ... (Transparenz)“	Transparenz
b) „... dürfen nur für festgelegte und legitime Zwecke erhoben werden ... (Zweckbindung)“	Nichtverketzung
c) „... Müssen auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein (Datenminimierung)“	Datenminimierung
d) „... personenbezogene Daten, die im Hinblick auf die Zwecke der Verarbeitung unrichtig sind, müssen unverzüglich gelöscht oder berichtigt werden.“	Intervenierbarkeit
e) „... dürfen nur so lange wie zur Verarbeitung erforderlich verarbeitet werden ...“	
f) „... Schutz vor Verlust ... Integrität und Vertraulichkeit“	Verfügbarkeit Integrität Vertraulichkeit



Im Zentrum steht die Verarbeitung.
Ohne Verarbeitung kein Risiko und keine Notwendigkeit an Maßnahmen.

Subverarbeitungen von personenbezogenen Daten gem. Art. 4 Nr. 2 DSGVO („und/oder“ aufgelöst)	Elementare Verarbeitungsvorgänge gemäß Art. 4 Nr. 2 DSGVO	Gruppen von Verarbeitungsvorgängen	Phasen der Datenverarbeitung	Kommentar
1 Erheben	1 Erheben	1 Sammeln (Sn) (erheben, erfassen, zudem auch erhalten und erzeugen)	1 Kollektion (Ko)	Rohdaten natürlicher Personen („Betroffener“) befinden sich in der Obhut eines Empfängers („Verantwortlicher“) Beispiele: Daten elektronisch abrufen, Unterlagen anfordern, Personen befragen, Internetsuche, aufschreiben oder aufnehmen von Daten
2 Erfassen	2 Erfassen			
3 Organisation	3 Organisation	2 Aufbereiten (Ab) (organisieren, ordnen)	2 Bereithaltung (Bh)	Diese Daten werden geordnet abgespeichert und sind in einem verarbeitungsfähigen Zustand verfügbar. Hinweis: Aufbau einer Struktur (simpel oder komplex ist unerheblich) Auch die Aufbewahrung einer Gewebeprobe kann hierunter fallen.
4 Ordnen	4 Ordnen			
5 Speicherung	5 Speicherung	3 Aufbewahren (Aw) (speichern, zudem auch ablegen von Papierdokumenten)		
6 Anpassung	6 Anpassung oder Veränderung	4 Bearbeiten (Ba) (anpassen, verändern)		
7 Veränderung				
8 Auslesen	7 Auslesen	5 Benutzen (Bn) (auslesen, abfragen, zudem auch filtern und auswerten)	3 Nutzung (Nu)	Die Daten sind für eine rechtskonforme und sachgemäße Verarbeitung, ggfs. auch für befugte Dritte, zugänglich. Sie können mit anderen Verarbeitungen verknüpft und der Zugang zu ihnen eingeschränkt werden. anpassen/verändern: inhaltliche Umgestaltung auslesen: vorhandener Datensatz wird genutzt (intern) abfragen: externe Datenbank wird genutzt verwenden: alle Arten des zweckgerichteten Gebrauchs oder der internen Nutzung Beispiele Offenlegung (11 bis 13): Datenweitergabe mündlich, schriftlich, elektronisch, Webseite oder Internet-Forum. Weitergabe innerhalb der Stelle ist Verwendung. Abgleich: Überprüfung, ob Daten von Betroffenen in mehreren Dateisystemen konsistent sind; Abgleich auch, wenn zu prüfen ist, ob bestimmte Daten in zwei unterschiedlichen Dateien vorhanden sind (z.B. welche Personen sind an mehreren Sachverhalten beteiligt) Verknüpfung: zusammenführen von Betroffenen Daten aus mehreren Dateisystemen oder Verknüpfung von mehreren Betroffenen über ein verbindendes Merkmal. einschränken: Reduzierung auf berechtigten Nutzerkreis; Sperrung
9 Abfragen	8 Abfragen			
10 Verwendung	9 Verwendung			
11 Offenlegung durch Übermittlung	10 Offenlegung durch Übermittlung	6 Bereitstellen (Bt) (Offenlegung durch Übermittlung, verbreiten oder andere Form des Bereitstellens)		
12 Verbreitung	11 Verbreitung oder eine andere Form der Bereitstellung			
13 andere Form der Bereitstellung				
14 Abgleich	12 Abgleich oder Verknüpfung	7 Zusammenführen (Zf) (abgleichen)		
15 Verknüpfung				
16 Einschränkung	13 Einschränkung	8 Einschränken (Es) (zudem auch sperren)		
17 Löschen	14 Löschen oder Vernichtung	9 Beseitigen (Bs) (löschen, vernichten)	4 Beseitigung (Bx)	Daten werden irreversibel entfernt oder physikalisch vernichtet. Behörden müssen vor der Löschung Archivwürdigkeit abklären!
18 Vernichtung				

Artikel 4 Nr. 2 DSGVO definiert den Begriff *Verarbeitung*. Diese Begriffsbestimmung dient dem SDM als Grundlage.

Die Zusammenfassungen in Gruppen von Verarbeitungstätigkeiten und Phasen der Datenverarbeitung erleichtert die vollständige Erfassung einer Verarbeitung (siehe Schaubild auf Seite 38 unten).

Je nach Bestimmung der Verarbeitung (in Gruppen von Verarbeitungstätigkeiten oder Phasen der Datenverarbeitung) erfolgt eine Zuordnung der zu prüfenden Verarbeitungsschritte nach Ebenen, wie das folgende Beispiel der Verarbeitung in einer Poststelle veranschaulicht (Tabelle unten).

In vielen Unternehmen und Behörden sind Poststellen vorhanden, deren Verarbeitung wichtig und nicht zu unterschätzen ist.

Art der Verarbeitung Beschreibung Phasen der Datenverarbeitung oder in Gruppen von Verarbeitungstätigkeiten	Ebene 1 (Fachebene) Aufgabe und Daten [Geschäftsprozess mit einem bestimmten funktionalen Ablauf; Bestimmung der für die Verarbeitung erforderlichen pBd sowie gesetzlichen Anforderungen; Definition von Rollen, Zuständigkeiten und Berechtigungen an den pBd. Aufgaben, Daten und Zwecke]	Ebene 2 Technische, organisatorische und personelle Prozesse [Praktische Umsetzung der Verarbeitung und des Zwecks; Sachbearbeitung und IT-Applikation (Fachapplikation eines Fachverfahren)]	Ebene 3 Infrastruktur (Räumlichkeiten, technische Systeme und Dienste) [IT-Infrastruktur; Bereitstellung von Funktionen für die Fachapplikationen der Ebene 2; technische Services; Betriebssysteme, virtuelle Systeme, Datenbanken etc., auch räumliche Gegebenheiten.]
Kollektion 1. Sammeln	Aufgaben: <ul style="list-style-type: none"> • Eingang und Ausgang von Postsendungen <ul style="list-style-type: none"> ◦ Briefe, Einschreiben, Pakete, Päckchen – alle Risikoklassen ◦ Brief vertraulich (an Hausleitung, Personalstelle, Personalrat, Datenschutz etc.) – Risikoklassen unbekannt • Annahme von elektronischen Nachrichten / E-Post (E-Mail, E-Rechnung, elektronische Anträge, Gerichtspost über besonderes elektronisches Behördenpostfach (beBPo) oder besonderes elektronisches Anwaltspostfach (beA)) Daten: Die Rechtsgrundlagen ergeben sich jeweils aus den Inhalten der Poststücke und umfassen sowohl Daten allgemein als auch besonders sensible Daten. Es gehen Poststücke aller Verarbeitungen durch die Poststelle, so dass die Einstufung „hohes Risiko“ gerechtfertigt ist. Abläufe: Eingang Briefe, Pakete, Päckchen: Vorsortieren in „zu öffnen“ und „nicht zu öffnen“; Eingang vermerken mit Eingangsstempel (tagesaktuell) Ausgang Briefe, Pakete, Päckchen: Mitnahme der Poststücke aus den Zustellbereichen Eingang Briefe vertraulich: Ungeöffnet vorsortieren und Eingang auf Umschlag vermerken mit tagesaktuellem Eingangsstempel Ausgang Briefe vertraulich: Mitnahme verschlossen aus Zustellbereich Eingang Einschreiben (zusätzlich zu Briefe u.a. – wie oben): Übergabe durch Postzusteller mit Auslieferungsbeleg elektronische Post: Gerichtspost: Eingang über elektronisches Behördenpostfach (beBPo) sonstige elektronische Post: Annahme und Sichtung	<ul style="list-style-type: none"> • Alle eingehenden und ausgehenden Poststücke werden durch die Beschäftigten der Poststelle in den dafür bereitgestellten Räumen mit eigener Schließanlage verarbeitet. Die Zugangsberechtigung besteht nur für Beschäftigte der Poststelle und für die Hausmeister. • Die Vorsortierung erfolgt mit Hilfe von Sortierregalen. • Zum Öffnen der Briefe werden elektronische Brieföffner verwendet. • Nicht zu öffnende Briefe, die irtümlich geöffnet (fehlerhafte Vorsortierung) wurden, werden wieder verschlossen und mit dem Vermerk „irtümlich geöffnet“ versehen. • Für elektronische Post und für Einschreiben steht ein Büroarbeitsplatz mit Standard-PC [Internet – Browser-, Office-Anwendungen (Word, Excel, Outlook)] zur Verfügung. Jede und jeder Beschäftigter erhält hierfür einen personalisierten Zugang. • Die Beschäftigten bringen einen Hinweis „Post“ an der Außenseite der Bürotür an, damit die Poststelle sieht, dass hier etwas mitzunehmen ist. Alternativ können Poststücke direkt bei der Poststelle in einem vorgegebenen Zeitfenster abgegeben werden. Übergabe erfolgt an der Türe, die nach Klingeln geöffnet wird. 	<ul style="list-style-type: none"> • Poststelle und Büroräume des Verantwortlichen • Gesamtes Betriebsgelände (für Transportwege) • Serviceleistungen Hausmeister, z. B. zum Transport von schweren Posteingängen • Technische Infrastruktur: <ul style="list-style-type: none"> ◦ Rechenzentrum intern ◦ Rechenzentrum extern (elektronische Poststelle, E-Rechnung, Gerichtspost) ◦ Auftragsverarbeiter für elektronische Anträge ◦ Deutsche Post für Datenaustausch bei Einschreiben und Paketen
Bereithaltung 2. Aufbereiten 3. Aufbewahren	Eingang: Aufbewahrung in offenen Regalfächer bis zur Verteilung Einschreiben: Abgleich der Poststücke mit Auslieferungsbeleg (der Post). Nach Prüfung Unterzeichnung mit Angabe von Klarnamen und eigenhändiger Unterschrift Aufbewahrung, Auslieferungsbeleg und Rückgabe am Folgetag an Postzusteller e-Post: Weiterleitung an zuständige Stellen (Fristen), direkt oder Funktionspostfach Ausgang: Aufbereiten zum Versand	<ul style="list-style-type: none"> • Nach Vorsortierung in Sortierregalen der Poststelle erfolgt die Übernahme der Papierpost in offene Transportboxen (gelb) • Für elektronische Post und für Einschreiben steht ein Büroarbeitsplatz mit Standard-PC [Internet – Browser-, Office-Anwendungen (Word, Excel, Outlook)] zur Verfügung. Jede und jeder Beschäftigter erhält hierfür einen personalisierten Zugang; Sichtung der eingehenden ePost erfolgt mehrmals täglich. • Für die Übernahme in die elektronische Akte wird die Papierpost mit Hilfe eines in der Poststelle befindlichen Scanners gescannt. • Versandvorbereitung für Postausgänge: kuvertieren, frankieren und für die Mitnahme durch Postzusteller am Folgetag vorbereiten • Einschreiben: <ul style="list-style-type: none"> • Briefumschlag wird gelabelt mit einem Klebeetikett (geliefert von Post); Inhalt: Sendungsnummer, QR-Code und Ankreuzmöglichkeit der Einschreibart; Praxis:ausschließlich Rückschein • Erfassung in Excel-Liste mit folgenden Feldern: Absender mit Anschrift und Kundennummer, Tagesdatum, Anzahl der Sendungen, Sendungsnummer, Name 1, Name 2, Straße, PLZ, Ort, Land, Einschreibart • Einlieferungsliste der Deutschen Post (VGA 1153/LI) wird ausgefüllt: Absender mit Anschrift und Kundennummer, Einschreibart national (Ankreuzfelder), Einschreibart international (Ankreuzfelder), von: erster Barcode, bis: letzter Barcode, Anzahl, Einlieferungsdatum, Gesamtzahl eingelieferter Sendungen • Aufbewahrung der versandfertigen Poststücke erfolgt separiert in der Poststelle bis zur Abholung durch einen oder einer Beschäftigten der Post. • Gescanntes Schriftgut (Originale) separiert für 4 Wochen (für etwaige Rückfragen) in der Poststelle aufbewahrt. 	<ul style="list-style-type: none"> • Poststelle und Büroräume des Verantwortlichen • Gesamtes Betriebsgelände (für Transportwege) • Technische Infrastruktur: <ul style="list-style-type: none"> ◦ Rechenzentrum intern ◦ Rechenzentrum extern (elektronische Poststelle, E-Rechnung, Gerichtspost) ◦ Auftragsverarbeiter für elektronische Anträge ◦ Deutsche Post für Datenaustausch bei Einschreiben und Paketen
Nutzung 4. Bearbeiten 5. Benutzen 6. Bereitstellung 7. Zusammenführen 8. Einschränken	Eingang: Die sortierten Poststücke werden nach Route gestapelt und anschließend verteilt. Ausgang: Übergabe der Poststücke an Postzusteller	<ul style="list-style-type: none"> • Die Postboxen werden mit einer Sackkarre transportiert. Während der Bereitstellung bleibt eine Person in der Poststelle. • Die Zustellung erfolgt in Postzimmern der Organisationseinheiten durch Ablage in offenen Regalfächern oder persönlich (hier insbesondere vertrauliche Post) • Für elektronische Post und für Einschreiben steht ein Büroarbeitsplatz mit Standard-PC [Internet – Browser-, Office-Anwendungen (Word, Excel, Outlook)] zur Verfügung. Jede und jeder Beschäftigter erhält hierfür einen personalisierten Zugang. • Gerichtspost: Eingang über besonderes elektronisches Behördenpostfach (beBPo) oder besonderes elektronisches Anwaltspostfach (beA), sofortige Weiterleitung an zuständige Stelle (Fristen!) • E-Mail, E-Rechnung oder elektronischer Antrag: Weiterleitung an zuständige sachbearbeitende Stelle (direkt oder Funktionspostfach) mehrmals täglich • Der Scan der Poststücke wird nach Kennzeichnung mit QR-Code über Outlook automatisiert elektronisch weitergeleitet. • Einschreiben: Übergabe an Postzusteller wird quittiert, Einlieferungsbeleg, Ablage in Papier in Ordnern, die in offenen Regalen abgestellt sind. 	<ul style="list-style-type: none"> • Poststelle, Postzimmer und Büroräume des Verantwortlichen • Gesamtes Betriebsgelände (für Transportwege) • Serviceleistungen Hausmeister, z. B. zum Transport von schweren Posteingängen • Technische Infrastruktur: <ul style="list-style-type: none"> ◦ Rechenzentrum intern ◦ Rechenzentrum extern (elektronische Poststelle, E-Rechnung, Gerichtspost) ◦ Deutsche Post für Datenaustausch bei Einschreiben und Paketen
Beseitigung Beseitigen	<ul style="list-style-type: none"> • Durch Bereitstellung an die jeweiligen Adressaten • erübrigt sich die Frage der Löschung für Papierpost. • Die übrigen Poststücke sind nach einer Aufbewahrungs- und Löschrfrist datenschutzkonform zu löschen. 	<ul style="list-style-type: none"> • Gescannte Poststücke (Originale in Papier) werden nach Ablauf der Aufbewahrungsfrist über einen Auftragsverarbeiter datenschutzkonform vernichtet. • Post: Löschung der weitergeleiteten Nachrichten 	<ul style="list-style-type: none"> • Poststelle des Verantwortlichen • Technische Infrastruktur: <ul style="list-style-type: none"> ◦ Rechenzentrum intern ◦ Rechenzentrum extern (elektronische Poststelle, E-Rechnung, Gerichtspost) ◦ Auftragsverarbeiter für Entsorgung Datenmüll ◦ Deutsche Post für Datenaustausch bei Einschreiben und Paketen

Nahezu alle Poststücke kommen hierüber in den Betrieb hinein und gehen heraus. Die Kategorien der Betroffenen und Daten umfassen alle Verarbeitungstätigkeiten.

Zu den haptischen Poststücken kommt die elektronische Post hinzu. Die sich ergebenden Verarbeitungsschritte wurden in einem Interview in einer behördlichen Poststelle aufgenommen und werden entsprechend dem SDM auf drei Ebenen abgebildet. Die Beschreibung erfolgt in vier Phasen der Datenverarbeitung.

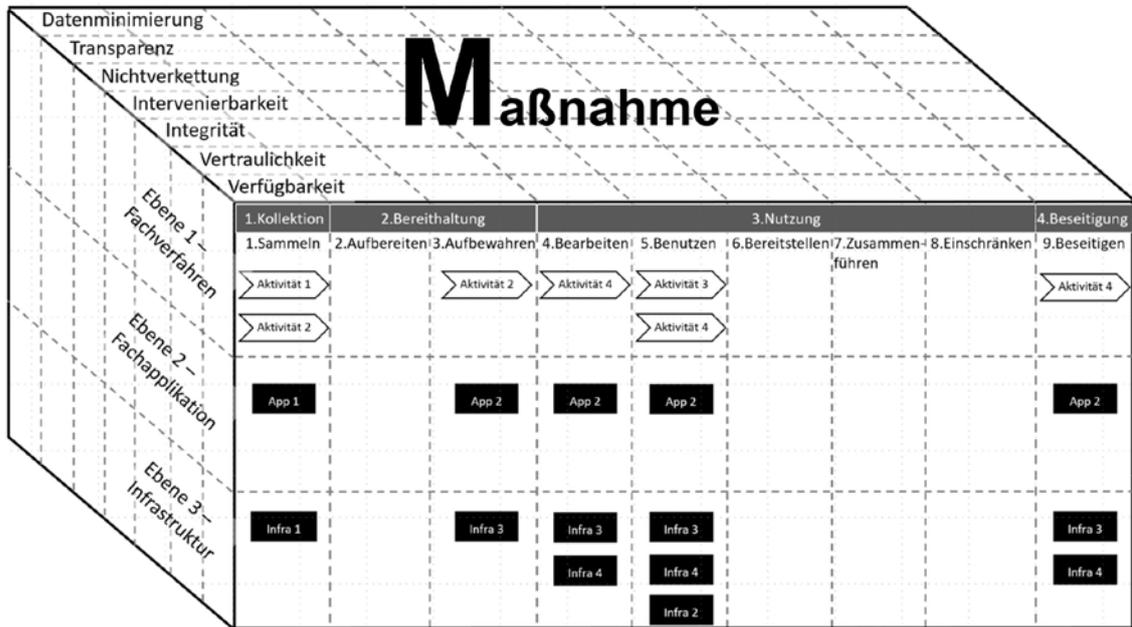
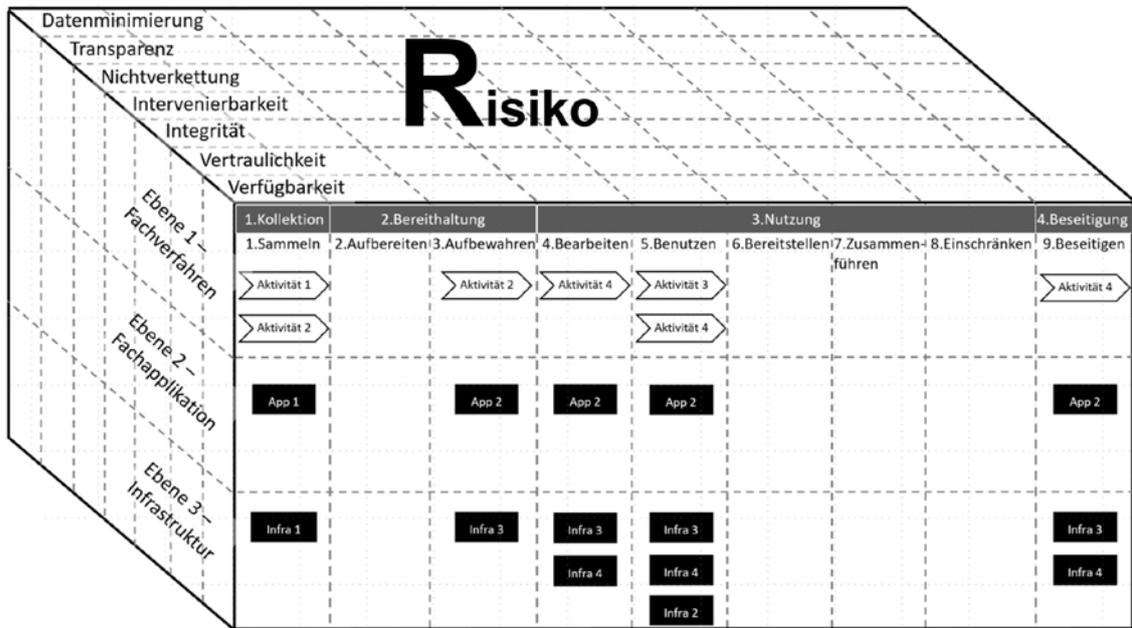
Die Zuordnung zu den Ebenen sollte nicht überzogen streng erfolgen. Wesentlich ist die vollständige Erfassung aller Verarbeitungsschritte, die fortschreitend angepasst werden. Der PDCA-Zyklus gehört dabei ganz selbstverständlich zum SDM, denn das Lernen und Verbessern sind Teil dessen.

Nach der Zuordnung der Ebenen zu den Verarbeitungsschritten erfolgt im nächsten Schritt ein In-Beziehungsetzen zu den sieben Gewährleistungszielen, die in Analogie zu Artikel 5 Absatz 1 DSGVO das *normative Gravitationszentrum* des SDM bilden.

In der dreidimensionalen Grafik sind die Phasen der Datenverarbeitung auf der Y-Achse und die Verfahrensebenen auf der X-Achse abgebildet. Der dreidimensionale SDM-Würfel bildet die Ebenen auf der Z-Achse, die Verarbeitungsphasen oder Verarbeitungsgruppen auf der Y-Achse und die Gewährleistungsziele auf der X-Achse ab.

Die Daten werden zunächst mit den Risiken dargestellt. Dann erfolgt auf den gleichen Achsen (die Achsen Z und Y bleiben unverändert) die Modellierung der Maßnahmen. Anhand des nachstehenden Bildes wird die Beziehung von Risiken und Maßnahmen deutlich.

Nimmt man jeweils die drei Seiten und steckt sie zusammen, so erhält man einen Würfel, den SDM-Würfel, der damit alle notwendigen Informationen enthält zum Verständnis von Verarbeitungsphasen, Verarbeitungsbeteiligten und den Risiken, so wie es die DSGVO erwartet.



Datenschutzfolgenabschätzung (DSFA)

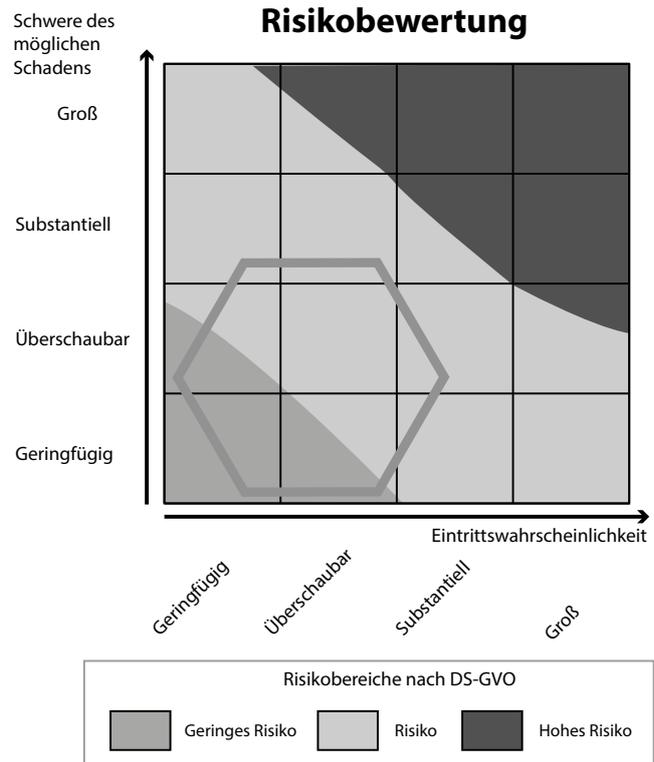
Im Falle der Verarbeitungen in der Poststelle wird aufgrund der Vielzahl unterschiedlicher Daten- und Betroffenen-Kategorien voraussichtlich ein hohes Risiko unterstellt. Auf eine Prüfung nach der Leitlinie zur Datenschutzfolgenabschätzung (DSFA) gemäß WP 248 Rev.01 der Datenschutzgruppe nach Artikel 29⁷ und den ergänzenden Orientierungshilfen der DSK zu Artikel 35 DSGVO in Form von Kurzpapieren (Nr. 5 und Nr. 18)⁸ wird an dieser Stelle verzichtet.

Eine Betrachtung der verschiedenen Ebenen lässt eine Gesamtbeurteilung aller möglichen Risikoquellen zu. Gerade die dreidimensionale Betrachtung öffnet die Augen. Kritiker könnten nun einwenden, es genüge allgemeine Schutzmaßnahmen zu installieren, die bei hohem Risiko etwas verschärft würden. Was aber sind allgemeine Schutzmaßnahmen und wie sähe die Verschärfung aus, wenn nicht alle Teilschritte einer Verarbeitung bekannt sind? Die Detailtiefe des SDM verschafft den nötigen Überblick.

Die Erstellung einer Datenschutzfolgenabschätzung nach SDM offenbart versteckte Risiken dadurch, dass die einzelnen Arbeitsschritte auf die miteinander verwobenen drei Ebenen sichtbar gemacht werden. Gerade die Hilfsmittel – in der Regel Anwendungen und Schnittstellen – sowie die Infrastruktur stehen regelmäßig im Kontext der jeweiligen Verarbeitung nicht im Fokus. Den Anwendenden fehlt häufig das Bewusstsein dafür. Bei der Aufnahme der Verarbeitungsschritte wird es vermittelt.

Zu den Risiken (vgl. auch CON.2 – BSI-Grundschutz) ist eine Abschätzung der Folgen zur vorgesehenen Verarbeitung zu erstellen (Artikel 35 Absatz 1 DSGVO). Dabei wird unterstellt, dass keinerlei Maßnahmen vorhanden sind. Nur in dieser „Blöße“ werden Risiken sichtbar. Naturgemäß zeigt die Risikobewertung hier einen hohen Ausschlag.

Nach der Modellierung der Maßnahmen, zu denen das SDM generische Maßnahmen und „Bausteine“ anbietet, zeigt sich ein rechtlich vertretbares Risiko. Eine risikofreie Verarbeitung ist nicht anzunehmen.



schwerpunkt

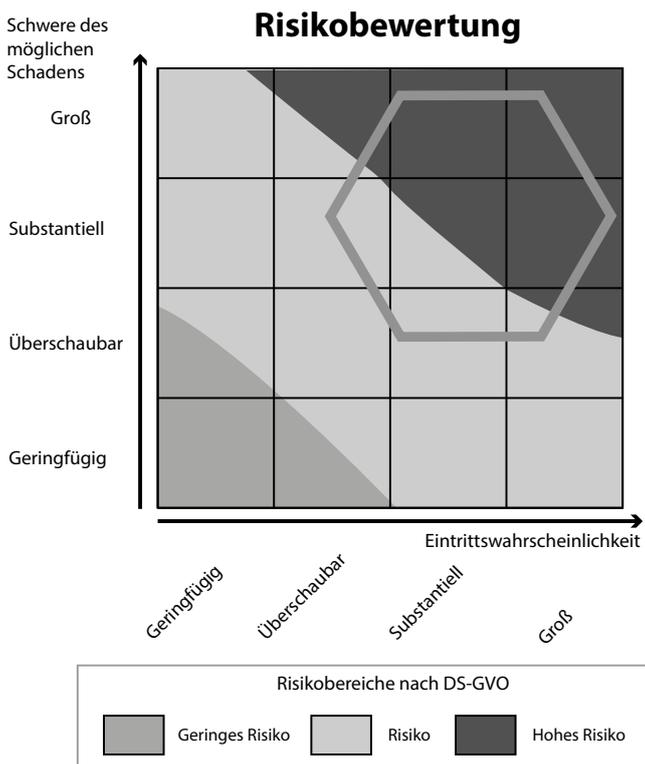
Was ein rechtlich vertretbares Risiko ist, bedarf der individuellen Festlegung.

Um die Eintrittswahrscheinlichkeit einschätzen zu können, ist die Erfassung von Datenschutzverletzungen nach Artikel 33 DSGVO – auch die der Nichtmeldungen – äußerst wertvoll, ansonsten kann die Einstufung als *gefühlte Wirklichkeit* qualifiziert werden. An dieser Stelle wäre Hilfe durch die Aufsichtsbehörden sinnvoll. Dort könnten die Erkenntnisse gebündelt pseudonymisiert zur Verfügung gestellt werden. Aus der Gesamtmenge ließen sich belastbare Schlüsse ziehen.

Die Datenschutzfolgenabschätzung schließt mit einem Bericht ab, der die erforderlichen Schutzmaßnahmen als Soll-Werte für die Verarbeitung vorgibt. Diese Soll-Werte sind mit dem IST abzugleichen. Im Idealfall gibt es Übereinstimmung. Abweichungen lösen Handlungsbedarf aus. Die anschließende Umsetzung ist zu überwachen.

Im Falle der Verarbeitungen der Poststelle ergaben sich folgende besonders wesentliche *versteckte Risiken*, die der Anpassung bedürfen:

- Der Abgleich mit bestehenden organisatorische Regelungen zeigte, dass diese nur selektiert (beispielsweise ohne besondere Postfächer) regelten, zum Teil mit anderen organisatorischen Maßnahmen kollidierten und das schlicht Regelungen fehlten.
- Die elektronische Post wird zunehmen und dabei erhält das Löschen besondere Beachtung. E-Post kommt an, wird wei-



tergeleitet. Die Speicherung erfolgt unter *Senden* und – sofern täglich gelöscht wird – unter *Löschen*. Ein Löschkonzept gemäß SDM-Baustein 60⁹ fehlt.

- Das Scannen wird gerade in der Umstellungsphase auf die elektronische Akte viel Zeit in Anspruch nehmen. Veränderungen benötigen Ressourcen. Eine personelle Verstärkung ist nicht vorgesehen.
- Das Zustellen mit Sackkarre birgt das Risiko, dass während der Ablage der Posteingänge und/oder Mitnahme von Poststücken für kurze Zeit keine Kontrolle besteht.
- Die Zustellung in den Postzimmern findet in offenen Regalsystemen statt. Damit verläuft das Rollen- und Rechtekonzept, wonach nur den Berechtigten die Inhalte offenbart werden dürfen, ins Leere. Vorgeschlagene Schutzmaßnahme: Installation von $\frac{3}{4}$ -Türen mit einem personalisierten Zugang, der deckungsgleich ist mit dem Rollen- und Rechtekonzept.
- Die technischen Unterstützungsmöglichkeiten eines Auftragsverarbeiters waren nicht bekannt.
- Die Möglichkeiten von Hilfsmitteln (hier Anwendungen) waren nicht hinreichend bekannt. Schulungsbedarf wurde offensichtlich.

Die Anwendung des SDM wirkt für Ungeübte zunächst kryptisch und sperrig. Warum so viele Informationen in solcher Detailtiefe? Wo ist der Mehrwert? Von außen betrachtet erinnert die detaillierte Abbildung der Verarbeitung an BPMN (Business Process Model and Notation), wonach Abläufe in *Swimlanes* grafisch dargestellt werden. Und damit kommen wir zum Mehrwert. Wer bereits Prozessbeschreibungen hat, die in besonders deutlicher Form der von der DSGVO verlangten „Beschreibung einer Verarbeitungstätigkeit“ entgegenkommen, kann diese nutzen. Sind solche (noch) nicht vorhanden, kann die Datenschutzerklärung nach SDM hierfür verwendet werden. Unterstützend können diese Dokumentation zudem für Stellenbewertungen oder Anpassungen im Arbeitsschutz genutzt werden. Es steckt also jede Menge Synergiepotenzial darin.

Kritik ist dennoch angebracht. Das SDM steckt noch in der Entwicklung. So wird zu den Gewährleistungszielen Verfügbarkeit, Vertraulichkeit und Integrität gerne auf den BSI-Grundschutz verwiesen. IT-Sicherheit schützt aber die Organisation, die Sicht der Betroffenen wird dabei nicht eingenommen. Das ist Aufgabe des Datenschutzes. Dieser Perspektivwechsel muss vollzogen werden. Ein weiterer Kritikpunkt ist, dass zu den übrigen Gewährleistungszielen noch nicht ausreichende Bausteine zur Verfügung stehen.

Die vorhandenen Bausteine müssen überarbeitet werden. Die Entwicklung der Methode hatte offensichtlich Vorrang vor der Anpassung der Bausteine an methodisch wesentliche Strukturen. Um zur Verbesserung und Annahme des SDM beizutragen, wurde die *User Group SDM e. V.* (zu finden unter UGSDM e. V. im Internet) gegründet. Hier arbeiten bundesweite Experten aus unterschiedlichen Branchen, wie Kanzleien, Wirtschaft, Informatik, Rechenzentrum und Behörden an einer Verbesserung und Erweiterung des SDM und nehmen Kenntnisse aus der Praxis gebührend auf.

Resümee

Datenschutz ist mitnichten ein Verhinderer. Ja, es bedarf der fachlichen Expertise, wie in allen sonstigen Fachlichkeiten von Organisationen auch. Das Standard-Datenschutzmodell bietet dabei eine Reihe von Standard-Maßnahmen an, die fortschreitend aktualisiert und erweitert werden. Bei einer zweckmäßigen Anwendung des SDM lässt sich für jede Organisation Datenschutz gut handhaben. So wird Datenschutz zum unterstützenden *Begleiter*.

Anmerkungen

- 1 *INFO1.pdf / bund.de* (https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Broschueren/INFO1.pdf?__blob=publicationFile&v=16), für Kinder zudem: *BfDI – Pixi Videos / bund.de* (<https://www.bfdi.bund.de/DE/Service/Mediathek/Pixi/Pixi-node.html>)
- 2 *Standard-Datenschutzmodell – Der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern / datenschutz-mv.de* (<https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/>)
- 3 *Protokoll_107_DSK.pdf / datenschutzkonferenz-online.de* (https://www.datenschutzkonferenz-online.de/media/pr/Protokoll_107_DSK.pdf)
- 4 *Beschluss 2020/06 – Standard-Datenschutzmodell | IT-Planungsrat* (<https://www.it-planungsrat.de/beschluss/beschluss-2020-06>)
- 5 *CON.2 Datenschutz / bund.de* (https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2023/03_CON_Konzepte_und_Vorgehensweisen/CON_2_Datenschutz_Edition_2023.pdf?__blob=publicationFile&v=3)
- 6 *Landesrecht BW – 1 O 93/23 | LG Mannheim 1. Zivilkammer | Urteil | Darlegung geeigneter technischer und organisatorischer Maßnahmen zur Gewährleistung angemessenen / landesrecht-bw.de* (<https://www.landesrecht-bw.de/bsbw/document/NJRE001569921>)
- 7 https://www.lfd.niedersachsen.de/startseite/infothek/edsa_leitlinien/vom-edsa-bestaetigte-leitlinien-158964.html
- 8 <https://www.datenschutzkonferenz-online.de/kurzpaepiere.html>
- 9 *SDM-V2.0_Löschen_und_Vernichten_V1.0a / datenschutz-mv.de* (https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/Bausteine/SDM-V2.0_L%C3%B6schen_und_Vernichten_V1.0a.pdf)



Karin de Lange

Karin de Lange, Komm. Dipl., behördliche Datenschutzbeauftragte (DSB) seit ca. 20 Jahren, *UDIS*-zertifiziert (udis zert 13070508), Dozentin an der *Verwaltungsakademie Bordsesholm (VAB)* u. a. Datenschutz, Gründungsmitglied des *User Group Standard Datenschutzmodell (UGSDM e. V.)* und Vorsitzende des *AK TOM UGSDM e. V.*

Warum Checklisten im Datenschutz kaum noch sinnvoll sind.

Besser: „einfach.SDM.machen“

Der Datenschutz hat sich in den letzten Jahren zu einem zentralen Anliegen für Unternehmen und Organisationen entwickelt. In einer Ära, die von Digitalisierung und zunehmend komplexen IT-Strukturen geprägt ist, stellt sich die Frage, wie Datenschutz effektiv gewährleistet werden kann. Traditionelle Methoden, wie beispielsweise Checklisten, haben sich lange als praktikable Werkzeuge erwiesen. Doch in der heutigen dynamischen und oft dezentralen IT-Landschaft stoßen diese schnell an ihre Grenzen. Dieser Artikel möchte aufzeigen, warum Checklisten im Datenschutz zunehmend ineffektiv werden und warum das Standard-Datenschutzmodell (SDM) eine überlegene Methode zur Bewertung und Dokumentation des Datenschutzes darstellt.

Herausforderungen moderner IT- und Datenverarbeitungslandschaft

Die IT- und Datenverarbeitungslandschaft hat sich drastisch gewandelt. Heute werden die Systeme nicht mehr ausschließlich intern verwaltet, sondern oft an Dienstleister ausgelagert oder als *Software-as-a-Service* (SaaS) implementiert. Diese Dienstleistungen werden individuell konfiguriert, was eine standardisierte Überprüfung durch einfache Checklisten erschwert. Moderne IT- und Datenverarbeitungslandschaft erfordern eine tiefere und umfassendere Analyse der Datenschutzmaßnahmen in den einzelnen Phasen und Ebenen der Verarbeitung.

Grenzen von Checklisten

Lange Zeit galten Checklisten als ein effektives Instrument, um die technischen und organisatorischen Maßnahmen (TOM) zur Gewährleistung des Datenschutzes schnell zu überprüfen. In einer Ära, in der Verarbeitungssysteme hauptsächlich inhouse verwaltet und zentral betreut wurden, bot diese Methode eine ausreichende Übersicht und Kontrolle. Die einfache Abfrage von Compliance-Aspekten durch Checklisten bot in weniger komplexen (IT-)Umgebungen einen ausreichenden Überblick. Checklisten haben jedoch mehrere Schwächen, wenn es darum geht, die Umsetzung von Datenschutzanforderungen in heutigen Verarbeitungen zu erfassen:

Oberflächliche Betrachtung

Bei einer Überprüfung anhand allgemeiner Checklisten werden Maßnahmen oft nur oberflächlich bewertet. Es wird lediglich das Vorhandensein bestimmter Dokumente oder Prozesse im Unternehmen bestätigt, ohne deren Effektivität oder Umsetzungstiefe zu bewerten. Diese Herangehensweise kann dazu führen, dass kritische Lücken innerhalb einer Verarbeitung oder in einer einzelnen Verarbeitungsphase übersehen werden.

Statische Natur

Checklisten sind zudem häufig statisch und unflexibel. Sie können selten die spezifischen Bedürfnisse und Besonderheiten der jeweiligen IT-Infrastruktur und Datenverarbeitungsprozesse abbilden, ohne die Checkliste aufwändig anzupassen und zu aktualisieren. Moderne IT-Umgebungen sind jedoch dynamisch und ändern sich ständig,

sind oft hybrid oder vollständig ausgelagert (Cloud-Dienste, SaaS-Anwendungen). Neue Technologien, Software-Updates und sich ändernde Geschäftsanforderungen erfordern eine flexible und anpassungsfähige Herangehensweise an den Datenschutz.

Standard-Datenschutzmodell (SDM)

Das SDM ist hier wesentlich flexibler. Die Methodik des SDM adressiert die Diversität und Komplexität moderner IT-Umgebungen durch eine detaillierte und spezifische Untersuchung der technischen und organisatorischen Maßnahmen zur Gewährleistung des Datenschutzes.

Die SDM-Methodik fragt, ob eine Maßnahme ausreichend und wirksam in allen Phasen der jeweiligen Verarbeitung entsprechend dem Risiko und der Eingriffsintensität umgesetzt ist – je Gewährleistungsziel.

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder hat am 24. November 2022 mit der Version 3.0 eine überarbeitete Version des Standard-Datenschutzmodells (SDM) verabschiedet. Die rechtlichen Anforderungen der Datenschutzgrundverordnung (DSGVO) werden vom SDM vollständig erfasst und mit Hilfe der Gewährleistungsziele systematisiert.

Mit dem SDM stellt die Konferenz ein Werkzeug bereit, mit dem die risikoadäquate Auswahl und rechtliche Bewertung der von der DSGVO geforderten technischen und organisatorischen Maßnahmen unterstützt wird.

Die Anwendungsbereiche des Standard-Datenschutzmodells sind Planung, Einführung und Betrieb von Verarbeitungstätigkeiten, mit denen personenbezogene Daten verarbeitet werden (personenbezogene Verarbeitungen) sowie deren Prüfung und Beurteilung. Damit unterstützt das SDM Verantwortliche in Wirtschaft und Verwaltung, die von der DSGVO auferlegten Nachweis- und Rechenschaftspflichten zu erfüllen.

Mittlerweile liegt das SDM in der Version 3.1 vor. Diese Version wurde von der 107. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder am 14. Mai 2024 beschlossen (<https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/>).

Neben der DSK empfehlen weitere Stellen die Anwendung des SDM, welches auch in aktuellen Rechtsprechungen Erwähnung

findet: Der IT-Planungsrat, der die IT-Aktivitäten des Bundes, der Länder und Kommunen untereinander koordiniert, empfiehlt die Anwendung des SDM für sämtliche öffentliche Verwaltungen Deutschlands. Der IT-Grundschutz des BSI empfiehlt in seinem Datenschutzbaustein CON2 die Anwendung des SDM. Die katholische und die protestantische Kirche Deutschland lehnen sich mit dem *Kirchen-Datenschutzmodell* (KDM) ganz eng an das SDM an.

In einem aktuellen Urteil (Az. 1 O 93/23) des Landgerichts Mannheim vom 15. März 2024 wird sehr konkret auf die Anforderungen des SDM bzw. des Artikels 5 der DSGVO Bezug genommen. <https://www.landesrecht-bw.de/bsbw/document/NJRE001569921>. Der EuGH stellt im Urteil C/2024/598 vom 11. Juli 2024 fest, dass der bloße Verstoß gegen die Informationspflichten gemäß Artikel 13, 14 DSGVO eine rechtsverletzende Datenverarbeitung darstellt, weil Artikel 5 Absatz 1 lit. a) DSGVO Transparenz als Grundlage jeder Datenverarbeitung verlangt <https://curia.europa.eu/juris/document/document.jsf?text=&docid=288148&pageIndex=0&doclang=DE&mode=req&dir=&occ=first&part=1&cid=2253776>. Unternehmen müssen, um ihrer Rechenschaftspflicht nachzukommen, darlegen und beweisen, dass die getroffenen Sicherheitsmaßnahmen geeignet sind, ein angemessenes Schutzniveau zu gewährleisten. Das SDM bietet hier eine verlässliche und anerkannte Methode nicht nur zur Dokumentation, sondern auch zur Bewertung und Optimierung.

Unterstützung finden Verantwortliche auch im neu gegründeten Verein UGSDM e.V. (User Group SDM), dessen Motto *einfach. SDM.machen* lautet. Hierbei geht es um den praktischen Erfahrungsaustausch bei der Anwendung der Methodik des SDM.

SDM im Vergleich zu Checklisten

Das SDM geht weit über das einfache Abfragen von Compliance-Aspekten hinaus und ermöglicht eine detaillierte Bewertung und Dokumentation der Wirksamkeit von Maßnahmen in den spezifischen Verarbeitungsphasen einer Verarbeitung.

Dies wird in Anlehnung an den bewährten PDCA-Zyklus ausgestaltet. Der Datenschutz-PDCA-Zyklus umfasst die folgenden vier Phasen:



Thomas Werning

Thomas Werning ist seit 1998 als Unternehmensberater für lösungsorientierten Datenschutz, faires Internetmarketing und verantwortungsvolle Digitalisierung tätig. Er ist alleiniger Gesellschafter und Geschäftsführer der *werning.com GmbH* und Gesellschafter und Geschäftsführer der *MoeWe GmbH*.

Zu seinem Hintergrund gehören Ausbildungen zum Datenschutzbeauftragten, Datenschutzauditor, Informationssicherheitsmanager und Google Ads Trainer inklusive einiger Zertifizierungen (BvD, GDD) sowie mehrere Gastsemester in Rechts- und Informatikstudiengängen. Er lebt mit seiner Familie in Lage/Lippe, fährt einen Oldtimer und spielt gerne eine Runde Golf.

Wichtig ist für ihn der respektvolle Umgang mit den Daten von Menschen sowie die digitale Verantwortung im Unternehmen. Mit der Aktion 1-Prozent.de wird dieses im eigenen Unternehmen aktiv gelebt, indem von jeder Rechnung 1 % des Betrages für Organisationen gespendet wird, die sich für Menschenrechte und Demokratie einsetzen.

- *Plan*: Planen, Spezifizieren, Dokumentieren
- *Do*: Implementieren, Protokollieren
- *Check*: Kontrollieren, Prüfen, Beurteilen
- *Act*: Verbessern

Prinzipien des SDM

Das SDM basiert auf sieben grundlegenden Gewährleistungszielen die sich aus Artikel 5 DSGVO ableiten:

1. *Datenminimierung*: Die personenbezogenen Daten sollen dem Zweck der Verarbeitung angemessen und auf das nötige Maß beschränkt sein. Nicht benötigte Daten sollen so früh wie möglich gelöscht werden.
2. *Transparenz*: Betroffene, aber auch Verantwortliche sowie zuständige Kontrollinstanzen sollen erkennen können, welche Daten wann und wie für welche Zwecke verarbeitet werden.
3. *Nichtverkettung*: Es ist zu gewährleisten, dass personenbezogene Daten nicht zusammengeführt (verkettet) oder angereichert werden, besonders wenn sie für unterschiedliche Zwecke erhoben wurden.
4. *Intervenierbarkeit*: Betroffenen Personen wird das Recht auf Auskunft, Benachrichtigung, Berechtigung, Datenübertragung, Löschung und Einschränkung, sowie Rücknahme und Widerspruchsmöglichkeiten gewährt. Die Betroffenen sollen die Möglichkeit haben, in die Verarbeitung Ihrer Daten eingreifen zu können.
5. *Integrität*: Die Anforderung, dass informationstechnische Prozesse und Systeme die Spezifikationen kontinuierlich einhalten, die zur Ausübung ihrer zweckbestimmten Funktionen für sie festgelegt wurden. Daten bleiben unversehrt, vollständig und aktuell.
6. *Vertraulichkeit*: Es ist zu gewährleisten, dass keine unbefugten Personen Zugriff auf die personenbezogenen Daten haben oder sich beschaffen können.

7. **Verfügbarkeit:** Es ist zu gewährleisten, dass der Zugriff auf personenbezogene Daten und ihre Verarbeitung unverzüglich und dauerhaft (während der erforderlichen Verarbeitung) möglich ist und sie ordnungsgemäß im vorgesehenen Prozess verwendet oder wiederhergestellt werden können. Die Verfügbarkeit umfasst die Auffindbarkeit von Daten durch Datenmanagement-Systeme, strukturierte Datenbanken, Suchfunktionen und die Verwendung technischer Systeme.

Tiefgehende Analyse

Das SDM ermöglicht eine tiefgehende Analyse der Datenschutzmaßnahmen. Es prüft nicht nur das Vorhandensein bestimmter Dokumente oder Prozesse, sondern bewertet deren Umsetzung und Wirksamkeit.

Ein Beispiel ist die Passwortrichtlinie eines Unternehmens: Während eine Checkliste oft lediglich bestätigt, dass eine Richtlinie existiert, untersucht das SDM, wie diese Richtlinie implementiert und durchgesetzt wird und ob sie den aktuellen Sicherheitsstandards entspricht – und dies jeweils auf die konkrete Verarbeitungstätigkeit und sogar Verarbeitungsphase bezogen.

Transparenz und Verantwortlichkeit

Das SDM schafft Transparenz in den Datenverarbeitungsprozessen und fördert die Verantwortlichkeit innerhalb der Organisation. Alle Schritte aller Verarbeitungstätigkeiten werden klar dokumentiert und sind jederzeit nachvollziehbar. Dies ermöglicht es Unternehmen, Schwachstellen zu identifizieren und konkrete Maßnahmen zu deren Behebung zu ergreifen.

Wird die Methodik des SDM schon bei der Planung einer Verarbeitung berücksichtigt könne viele Fragestellungen, auch mit Mitarbeitervertretungen oder bei Einführung einer Betriebsvereinbarung, im Vorfeld geklärt und dokumentiert werden.

Flexibilität und Anpassungsfähigkeit

Das SDM ist flexibel und anpassungsfähig an die spezifischen Bedürfnisse und Besonderheiten der jeweiligen IT-Infrastruktur und Datenverarbeitungsprozesse, ohne die Methodik der Fragestellungen zu verändern. So lässt es sich auch auf individuellen Konfigurationen und Dienstleistungen anwenden, die in modernen IT- und Datenverarbeitungslandschaften eingesetzt werden. Durch die Festlegung von Eingriffsintensität und Risiko wird die getroffene Maßnahme dahingehend bewertet, ob sie entsprechend den Gewährleistungszielen ausreichend umgesetzt ist.

Fazit

In einer Welt, in der Datenschutz immer mehr an Bedeutung gewinnt und die IT-Umgebungen und Datenverarbeitungen zunehmend komplexer werden, reichen traditionelle Methoden wie Checklisten oft nicht mehr aus, um umfassenden Datenschutz zu gewährleisten und zu dokumentieren. Das Standard-Datenschutzmodell in der Version 3 bietet hier eine moderne, tiefgehende und effektive Methode, um diesen Anforderungen gerecht zu werden und die Grundrechte und Grundfreiheiten von Betroffenen zu schützen. Unternehmen, die diesen Ansatz verfolgen, sind besser aufgestellt, um auf die Herausforderungen in komplexen Verarbeitungen zu reagieren und das Vertrauen ihrer Nutzer und Kunden zu stärken. Mit dem SDM können Verantwortliche die Rechenschaftspflicht der DSGVO effektiv erfüllen (Artikel 5 (2) DSGVO – Rechenschaftspflicht).

Wissenschaft & Frieden 3/24

Widerstehen – Widersetzen

Zivilgesellschaftlicher Protest bricht sich immer wieder Bahn auf der Straße oder im Netz – Bürger:innen versuchen repressiver Gewalt unbewaffnet Einhalt zu bieten, Forderungen an bessere Verhältnisse durchzusetzen oder ein ungerechtes Regime zu kippen. Ziviler Widerstand und gewaltfreier Protest kommen in vielen Variationen vor.

Dazu stellen sich eine Reihe von Fragen: Wie kann Widerstand erfolgreich sein, und wo liegen die gesellschaftspolitischen Grenzen von Radikalität? Wie angemessen sind die Daten zur Analyse von Zivilem Widerstand? Wie formen die Weltbilder hinter bestimmten Bewegungen oder Widerstand-Leistenden auch deren Methoden und Aktionsformen? Antworten dazu gibt es im neuen Heft 3/24 von W&F.

Mit Beiträgen von *Jannis J. Grimm, Julia Nennstiel, Lilly Roll-Naumann, Rita Schäfer, María Cárdenas* und weiteren.

Weitere Schwerpunkte: *Bayer et al.* Militarisierung – Zeitgeist einer neuen Ära? | *Krüger* Nukleares Erbe in Kasachstan | *Eckerle* Präfigurative Friedenspsychologie



**W&F 2/2024 | August | 68
Seiten | 12 € (Druck) / 9 €
(ePUB+PDF)**
Bestellen unter:
www.wissenschaft-und-frieden.de

Chris Köver, Charlotte Horsch

„Kinder haben auch ein Recht auf Privatsphäre“

2. September 2024 – Die Hälfte aller Eltern von Kindern im Alter zwischen drei und 14 Jahren kann sich vorstellen, diese permanent zu orten. Hier erzählt die Medienpädagogin Charlotte Horsch, was das mit Kindern macht und wie Eltern mit ihren Ängsten umgehen können.

Wo ist mein Kind und was stellt es gerade an? Diese Frage stellen sich Eltern oft. Und wer es tatsächlich zu jedem Zeitpunkt ganz genau wissen will, kann das heute auch. Mit digitalen Kinderuhren oder Monitoring-Apps auf dem Handy können Eltern ihre Kinder rund um die Uhr verfolgen: Sie sehen den Standort, können kurze Nachrichten schicken oder bekommen einen Hinweis, wenn das Kind weiter läuft als bis zur nächsten Ecke.

Nahezu die Hälfte aller Eltern von Kindern im Alter zwischen drei und 14 Jahren konnten sich vorstellen, ihre Kinder permanent zu orten, fand die Verbraucherzentrale NRW in einer Befragung heraus¹. Aber welche Konsequenzen hätte das? Charlotte Horsch arbeitet am Institut für Medienpädagogik JFF in München und berät regelmäßig auch Eltern, die ihre Kinder tracken oder darüber nachdenken. Einer ihrer Schwerpunkte: Medienerziehung in der Familie.

netzpolitik.org: Charlotte Horsch, die Schule geht wieder los. Eltern fragen sich jetzt vielleicht, wie sie ihre Grundschul Kinder besser im Auge behalten können. Was raten sie Eltern, die ihr Kind mit Uhren oder Apps tracken wollen?

Charlotte Horsch: Ich kann das nachvollziehen. Vielleicht ist der Schulweg weiter. Die Kinder sind auf unbekanntem Strecken unterwegs und man möchte wissen, ob das Kind sicher angekommen ist. Da kann so ein Gerät eine gewisse Sicherheit vermitteln. Gleichzeitig möchte ich Eltern auffordern, noch mal drüber nachzudenken, wann Tracking sinnvoll ist und wie sie es einsetzen.

netzpolitik.org: Wie sollte man es denn einsetzen?

Charlotte Horsch: Nicht rund um die Uhr. Und auf keinen Fall heimlich. Kinder sollten Bescheid wissen, dass sie getrackt werden, wann die Eltern sie tracken und wann nicht.

netzpolitik.org: Warum ist das wichtig?

Charlotte Horsch: Weil Heimlichkeit dem Vertrauensverhältnis schadet. Wenn Kinder irgendwann erfahren, dass die Eltern die ganze Zeit gewusst haben, wo sie sich befinden, kann das zu einem massiven Vertrauensbruch führen. Zum anderen haben Kinder ein Recht darauf, das zu wissen. Kinder haben auch ein Recht auf Privatsphäre.

netzpolitik.org: Und warum raten sie davon ab, dass Eltern ihre Kinder rund um die Uhr tracken?

Charlotte Horsch: Die Kinder können dadurch den Eindruck bekommen: Meine Eltern vertrauen mir nicht oder ich kann das gar nicht alleine. Sie verlassen sich komplett auf den Schutz der Eltern und entwickeln wenig Eigenständigkeit. Deswegen möchte ich Eltern ermutigen, das Tracking, wenn überhaupt, sporadisch einzusetzen. Vielleicht für die ersten Wege, die allein bewältigt werden, aber nicht routinemäßig bei jedem Weg.

Und was mir am wichtigsten ist: Der technische Schutz kann keine Erziehung ersetzen.

netzpolitik.org: Das heißt?

Charlotte Horsch: Es ist für Eltern vielleicht verlockend, sich auf das Tracking als Schutz zu verlassen. Nach dem Motto: Wenn was passiert, weiß ich es ja. Das reicht aber nicht. Die Kinder müssen wissen: Wie verhalte ich mich in einer Situation, in der ich nicht weiter weiß? Was mache ich, wenn mich jemand auffordert mitzukommen? Oder wenn ich den Bus verpasst habe? Es geht darum, dass man den Kindern das zutraut und sie darin bestärkt, eigenständig in der Situation zu handeln.

Das Tracking, wenn es zum Einsatz kommt, sollte nur eine zusätzliche Komponente sein und kein Ersatz für die Erziehung der Eltern.

netzpolitik.org: Sie bieten auch Elternabende zu diesem Thema an. Was ist die Hoffnung der Eltern, wenn sie ihre Kinder mit solchen Uhren oder Apps ausstatten?

Charlotte Horsch: Das vermittelt ein Gefühl von Sicherheit. Ich hatte neulich eine Mutter auf einem Elternabend, die meinte: Wenn ich könnte, würde ich mein Kind auch chippen, aber ich darf ja nicht. Das Gerät vermittelt der Mutter: Wenn meinem Kind etwas passiert, kann ich ihm helfen.

„Die Sicherheit kann trügerisch sein“

netzpolitik.org: Stimmt das denn?

Charlotte Horsch: Klar kann das in bestimmten Situationen helfen. Vielleicht steigt das Kind in die falsche Bahn, landet irgendwo und weiß nicht weiter. Da hilft es, wenn ich anrufen kann und sagen: Ich hole dich jetzt ab. Aber die Sicherheit kann trügerisch sein. Kinder können die Geräte ja einfach abneh-

men, wenn sie das Tracking der Eltern umgehen möchten. Dann hängt das Kind die Uhr an den Zaun und bewegt sich trotzdem weiter weg, als es darf.

netzpolitik.org: *Sehen wie weitere Gefahren, die Eltern beim Einsatz dieser Geräte übersehen?*

Charlotte Horsch: Diese Geräte senden Daten und die sind häufig leicht hackbar. Entsprechend ist es wichtig, sich vorher zu informieren: Wo werden die Daten gesichert, wie werden die Daten gesichert? Das machen nicht alle Eltern.

netzpolitik.org: *Was könnten andere mit den Bewegungsdaten meines Kindes anstellen?*

Charlotte Horsch: Als wirklich schlimmsten Fall kann es sein, dass Personen, die den Kindern nicht wohlgesonnen sind, auf diese Daten zugreifen können. Die sehen dann genauso wie ich: Wo befindet sich mein Kind gerade.

netzpolitik.org: *Sie gehen auch regelmäßig in Grundschulklassen und sprechen mit den Kindern. Wie finden die Kinder, dass sie von den Eltern getrackt werden?*

Charlotte Horsch: Manche sagen: Ich finde das total gut, weil Mama Bescheid weiß und auf mich aufpasst. Andere fühlen sich überwacht und erzählen mir, wie sie die Uhr an den Zaun hängen, wenn sie den Schulhof verlassen. So etwas kann dazu führen, dass sich diese Kinder auch später nicht an die Eltern wenden, wenn ihnen etwas geschehen ist – weil sie dann zugeben müssten, dass sie ganz woanders waren. Das sehe ich auch in anderen Bereichen, etwa bei Online-Mobbing oder Cybergrooming ...

netzpolitik.org: *... wenn also Erwachsene sich Kindern im Netz mit sexuellen Absichten nähern.*

Charlotte Horsch: Auch hier können Kinder das Gefühl haben: Ich kann mich nicht an meine Eltern wenden, weil ich dann zugeben müsste, dass ich die Regeln umgangen habe und bestraft werde. Das kann dazu führen, dass die Kinder damit alleingelassen werden.

„Das Tracking wird salonfähiger“

netzpolitik.org: *Sie sagten, Kinder haben ein Recht auf Privatsphäre. Rein rechtlich dürfen Erziehungsberechtigte in Deutschland ihre Kinder digital überwachen – auch ohne deren Wissen*

und Zustimmung. Sollten Kinder ein Recht darauf haben, nicht von ihren Eltern überwacht zu werden?

Charlotte Horsch: Mit Kinderrechten ist es komplex. Kinder haben ein Recht auf Privatsphäre, gleichzeitig müssen Eltern den Schutz des Kindes gewährleisten. Für die Eltern ist das eine Abwägungsfrage: Ist der Schutz gerade wichtiger als das Recht auf Privatsphäre? Manche entscheiden sich dann für das Tracking.

netzpolitik.org: *Tracken Eltern ihre Kinder heute häufiger als vor fünf Jahren?*

Charlotte Horsch: Vor der Pandemie war das bei Elternabenden kein Thema, seit einigen Jahren schon. Ich habe den Eindruck, dass viele Eltern mehr Sorgen haben, dass dem Kind etwas zustoßen könnte. Zum anderen hat sich der Markt sehr erweitert. Es gibt heute verschiedenste Möglichkeiten Kinder zu tracken – von Smartwatches bis Apps, die verschiedene Kontrollmöglichkeiten bieten.

netzpolitik.org: *Wird das Tracking damit normaler?*

Charlotte Horsch: Es wird salonfähiger. Vor einigen Jahren haben weniger Eltern von sich aus berichtet, dass sie ihre Kinder tracken. Und es wurde von anderen Eltern kritisch beäugt. Jetzt dreht sich das um: Für viele Eltern ist es ganz selbstverständlich und die Skeptischen werden weniger.

„Diese Geräte verstärken oft die Sorgen der Eltern“

netzpolitik.org: *Mehr als die Hälfte der Kinder unter zehn Jahren wird heute noch von den Eltern in die Schule gebracht, andere tracken ihre Kinder digital. Was für ein Bild von Kindern steht dahinter?*

Charlotte Horsch: Der gesellschaftliche Umgang mit Kindern ist das eine. Aber vielleicht haben sich andere Dinge geändert: Wie viele Schulbusse gibt es noch auf dem Land? Wie oft müssen die Kinder vielleicht selber gefahren werden? Vielleicht haben sich die Wege tatsächlich verlängert oder sind gefährlicher geworden. Wodurch die Eltern das Gefühl haben, sie müssten ihre Kinder tracken. Gleichzeitig habe ich den Eindruck, dass diese Geräte die Sorgen der Eltern oft verstärken.

netzpolitik.org: *Wie das?*

Charlotte Horsch: Diese Geräte vermitteln immer die Möglichkeit, es könnte etwas passieren. Manche Eltern berichten mir,

Chris Köver und Charlotte Horsch

Chris Köver ist seit 2018 Redakteurin von *netzpolitik.org*. Sie recherchiert unter anderem zu Digitaler Gewalt, so genannter Künstlicher Intelligenz und zur Migrationskontrolle. Bis 2014 war sie Chefredakteurin des *Missy Magazine*². **Kontakt:** E-Mail³ (OpenPGP⁴).

Charlotte Horsch arbeitet für das *JFF – Institut für Medienpädagogik in Forschung und Praxis*.

dass sie das Tracking deswegen von sich aus wieder herruntergeschraubt haben. Weil sie gemerkt haben, dass es ihnen nicht guttut.

Eine Mutter hat mir berichtet, dass sie ganz unruhig war und ständig aufs Handy geschaut hat, wenn ihre Tochter unterwegs war. Die Mutter hat die App dann von ihrem Smartphone gelöscht hat und konnte nur noch auf einem Tablet sehen, wo sich ihre Tochter befindet.

netzpolitik.org: *Geht es in Ihren Workshops auch darum, wie Eltern mit ihren Ängsten um die Kinder umgehen könnten – auch ohne ihr Kind zu tracken?*

Charlotte Horsch: Ich bin offen den Eltern gegenüber, dass ich das Tracking sehr kritisch sehe, mit dem Blick darauf, was das mit den Kindern macht. Gleichzeitig versuche ich herauszufinden, woher die Sorgen kommen. Wo sind sie berechtigt und wo weniger rational?

Ich öffne dann die Runden und lasse Eltern miteinander reden. Da kommt es eigentlich immer zu kontroversen Diskussionen. Mir ist wichtig, dass nicht nur ich als die Medienpädagogin vorne stehe und den Eltern sage, wie sie es am besten machen. Das ist nämlich von der Familie abhängig. Jedes Kind ist anders, jede Familie ist anders. Das betrifft alle Bereiche der Mediener-

ziehung. Es gibt nicht den einen richtigen Weg, sondern man muss immer abwägen: Was funktioniert für uns?

netzpolitik.org: *Wie reagieren Eltern denn, wenn sie von den Folgen des Trackings für die Kinder sprechen?*

Charlotte Horsch: Manche verschließen sich dann und betonen, wie gut ihr Verhältnis zum Kind ist und wie groß das Vertrauen. Dass es für das Kind überhaupt kein Problem sei, dass die Mutter immer weiß, wo es sich aufhält. Andere kommen tatsächlich ins Nachdenken. Die kommen dann nach der Veranstaltung nochmal zu mir und stellen Fragen.

Quelle: <https://netzpolitik.org/2024/gps-tracker-fuer-kinder-kinder-haben-auch-ein-recht-auf-privatsphaere/>

Anmerkungen

- 1 <https://www.vzbv.de/pressemitteilungen/ortung-von-kindern-tracking-technik-spaltet-elternschaft>
- 2 <https://missy-magazine.de/online-magazin/>
- 3 <mailto:chris@netzpolitik.org>
- 4 <https://keys.openpgp.org/search?q=0x5E598DD0D37B9F71A88DD92233D38859243016F9>



Janine Malz

Der Wert menschlicher Übersetzung

1. September 2024 – *KI-generierte Übersetzungen von E-Mails, Nachrichtenartikeln oder Speisekarten sind für unsere Gastautorin überhaupt kein Problem. Aber bei literarischen Texten sollten allein Menschen Hand anlegen, argumentiert sie – und vor allem Buchverlage sollten von KI die Finger lassen.*

Vor Kurzem erreichte mich die E-Mail eines großen deutschen Verlags, der mich als Literaturübersetzerin aus dem Englischen, Italienischen und Niederländischen anfragte; ich sei ihnen wärmstens empfohlen worden. Es ging um eine vierteilige Romanreihe aus den Niederlanden. Die Romane seien kurzweilig, die Figuren charmant, und die Autorin schreibe mit Witz und Herz, so die Lektorin. So weit, so normal. Doch ich wurde nicht etwa für die Übersetzung angefragt, sondern nur als Prüferin für eine KI-generierten Übersetzung, sogenanntes Post-Editing.

Das Honorar: Fünf Euro pro Normseite – ein übliches Übersetzungshonorar liegt um die 20 Euro. Und ich sollte auch keinen Übersetzungsvertrag erhalten, sondern nur einen Redaktionsvertrag. Falls ich Bedenken hätte, würde man sich sonst auch über die Empfehlung einer Kollegin freuen. Mir fiel die Kinnlade herunter.

Übersetzen ist auch Beziehungsarbeit

Denn was diese scheinbar harmlose Anfrage beinhaltete, hieß nichts weniger als den Anfang vom Ende meines Berufs. Kurzerhand verfasste ich eine Antwort, in der ich nicht einfach

lapidar ablehnte, sondern erklärte, warum diese Entwicklung aus Übersetzerinnensicht fatal wäre. In der E-Mail ging ich auf folgende fünf Argumente ein:

1. Post-Editing heißt, für ein geringeres Honorar in kürzerer Zeit einen deutschen Text zu schustern. Selbst wenn ich mir Mühe gebe, würde am Ende ein Text herauskommen, der qualitativ schlechter ist als ein Text, den ich selbst erschaffe. Das liegt in der Natur der Sache: Sobald erst einmal etwas auf Deutsch dasteht, ist es schwer, sich davon zu lösen und auf eigene, idiomatische und kreative Lösungen zu kommen.
2. Post-Editing ist nur scheinbar ein Zeitgewinn: Wenn ich selbst übersetze, habe ich vor mir einen ausgangssprachlichen Text und meine unbeschriebene Word-Datei, in die ich meinen Text hineintippe. Beim Post-Editing muss ich aber erstmal den deutschen Output Satz für Satz mit dem Ausgangstext abgleichen, um Fehler zu entdecken und ausmerzen. Das kostet Zeit. Dann soll ich ja aber auch noch einen gut lesbaren, flüssigen Text daraus machen.
3. Übersetzen ist nicht nur Textarbeit, sondern auch Recherche: Wichtig ist, sich klar zu machen, dass die Maschine den

Text nicht versteht. Sie versteht keine Anspielungen, Wortspiele, Witze, Bezüge, sprechende Namen. Als Übersetzerin bin ich oft in engem Austausch mit den Autor:innen, frage nach, was sie mit bestimmten Formulierungen meinen, recherchiere Fakten nach und finde nicht selten Fehler im Original, weil in anderen Ländern teilweise das Lektorat nicht so gründlich ist wie bei uns.

4. Übersetzen ist nicht nur Textarbeit, sondern auch Beziehungsarbeit: Gerade den niederländischsprachigen Markt kennen wir Übersetzer:innen sehr gut und fungieren mitunter auch als Scouts, entdecken neue Bücher aus den Niederlanden und Flandern, bieten sie deutschsprachigen Verlagen an. Mitunter gehe ich mit meinen Autor:innen auch auf Lesereise, moderiere und dolmetsche das Gespräch. Das alles kann die KI nicht leisten. Ich kann das aber nur so lange leisten, solange ich von meiner Arbeit leben kann.
5. Es wird ein Redaktions-, kein Übersetzungsvertrag angeboten. Das heißt für mich, ich erlange keine Urheberrechte an dem deutschen Text, ergo erhalte ich auch keine Beteiligung seitens des Verlags am Nettoverkaufserlös und keine Bibliothekstantien durch die VG Wort. Das ist angesichts der bescheidenen Honorare aber ein wichtiger Baustein in meinem Einkommen. Außerdem ist die Frage, wer ist dann überhaupt Urheber an der deutschen Buchveröffentlichung? Das kann juristisch nur ein Mensch sein, keine Maschine.

Entwicklung bedroht die Kulturbranche

Übersetzen ist nicht nur ein Beruf, es ist Berufung. Meine Kolleg:innen arbeiten oft weit über eine normale 40-Stunden-Woche hinaus und tragen als Freiberufler:innen zusätzliche Risiken – niemand bezahlt uns, wenn wir krank oder im Urlaub sind. Das Durchschnittshonorar ist in den letzten Jahrzehnten inflationsbereinigt gesunken¹(!), viele bekommen eine so geringe Rente, dass sie auch im Alter weiter arbeiten müssen².

Warum wir das machen? Wir lieben unseren Beruf, wir lieben Literatur und setzen uns dafür mit all unserem Können und unserer Erfahrung ein. Wenn Verlage nun aus Kostengründen die Honorare weiter absenken, werden immer mehr Kolleg:innen in andere Berufe ausweichen, weil sie schlicht nicht mehr davon leben können. Damit geht all das verloren, was ich oben geschilbert habe.

Nachdem ich die E-Mail abgeschickt hatte, stellte ich die Anfrage und meine Antwort – nur unter Angabe des Verlags, aber ansonsten anonymisiert – bei Instagram ein, anschließend auch bei LinkedIn und Facebook. Was folgte, hat mich überwältigt. Mein Beitrag ging viral, wurde tausendfach gelikt und geteilt,

unter anderem von Schriftsteller:innen wie Saša Stanišić, Nicole Seifert und Nina George. Übersetzer:innen und Autor:innen, Journalist:innen, Sprecher:innen, Illustrator:innen und erfreulicherweise auch viele Leser:innen waren entsetzt und dankten mir für den öffentlichen Protest gegen eine Entwicklung, die die gesamte Kunst- und Kulturbranche bedroht.

Was es heißt, Literatur zu übersetzen

Überall wird der Rotstift angesetzt, gerade erst wurden Pläne bekannt, wonach im neuen Bundeshaushalt trotz gleichbleibendem Kulturetat ausgerechnet bei der freien Kunst- und Kulturszene drastisch gekürzt werden soll³ – den sechs Bundeskulturfonds, darunter dem Deutschen Übersetzerfonds, sollen die Mittel um die Hälfte (!) gestrichen werden. Für Übersetzer:innen ist das ein schwerer Schlag, denn diese Stipendien sind enorm wichtig in einem Beruf, in dem das Honorar gerade bei anspruchsvollen Werken den Zeitaufwand nicht abdeckt, sodass sie letztlich auch den Verlagen zugutekommen.

Was mir in der Debatte im Nachgang meines Online-Posts auffiel, ist, wie viele offenbar ein merkwürdiges Verständnis davon haben, was es heißt, Literatur zu übersetzen. Das mache ich erstmal niemandem zum Vorwurf, denn auch ich weiß ja nicht, was andere Leute in ihren Berufen so machen. Aber von einem Verlag würde ich das schon erwarten.

Sprachgefühl statt Sprachberechnung

KI-Technologie, die auf sogenannten großen Sprachmodellen beruht, wie DeepL oder ChatGPT, ist im Alltag sicherlich praktisch, etwa beim Übersetzen von Geschäftsmails oder Zeitungsartikeln oder beim Verständigen in einem fremdsprachigen Kontext. Aber in der Literatur haben wir es mit Texten zu tun, die über die reine Informationsvermittlung hinausgehen, bei denen Stil, Rhythmus und Klang eine essentielle Rolle spielen, die sprachlich erfinderisch und originell sind, eine eigene Handschrift tragen. Die Emotionen, Humor und kulturelle Eigenheiten transportieren. Die man womöglich immer wieder lesen und erfahren möchte – nicht nur einmal kurz überfliegen. Literatur ist Kunst.

Und ja, das trifft auch auf Unterhaltungsliteratur zu, denn auch dort will die Handlung kunstvoll verwoben, wollen Dialoge lebendig geschrieben und Figuren glaubwürdig ausgearbeitet sein.

KI-Sprachmodelle erstellen Texte anhand von Wahrscheinlichkeiten. Sie berechnen etwa, welches Wort am ehesten auf ein vorangegangenes folgt. Die Ergebnisse können teils beeindruckend sein.

Janine Malz

Janine Malz⁴ ist seit 2014 als freiberufliche Literaturübersetzerin tätig und übersetzt Belletristik und Sachbücher aus dem Englischen, Italienischen und Niederländischen ins Deutsche.

cken, aber sie können nicht die Konsistenz und Tiefe eines Texts erreichen, den ein Mensch übersetzt. Mit literarischem Schreiben hat das wenig zu tun. Es heißt ja auch „Sprachgefühl“, nicht „Sprachberechnung“. Literatur entspringt dem Bedürfnis des Menschen, sich gegenseitig Geschichten darüber zu erzählen, was es heißt, Mensch in dieser Welt zu sein. Zu glauben, eine Maschine – die nie in dieser Welt gelebt hat – könne das genauso gut übernehmen, ist gelinde gesagt grotesk.

Verlage, die von sich behaupten, Bücher zu lieben, sollten Literatur auch als das behandeln, was sie ist: eine durch und durch menschliche Ausdrucksform. Kein maschinell erzeugtes Ramschprodukt.

Martin Schwarzbeck

Wie Online-Pflicht Menschen ausschließt

31. August 2024 – Ab Sonntag kann man in Berliner Bussen nicht mehr bar bezahlen, für fünf Schwimmbäder gibt es nur noch Digitaltickets. Menschen wie Petra werden so zunehmend von der gesellschaftlichen Teilhabe ausgeschlossen. Aber mehrere Initiativen kämpfen für analoge Alternativen.

Samstagsvormittag vor dem Freibad am Insulaner in Berlin. Eine dreiköpfige Familie, vollgepackt mit Taschen, Kühlbox und Sonnenschirm, wird am Eingang von einem Sicherheitsdienstleitenenden gestoppt. Der Securitytyp tippt auf einen Aufsteller. Darauf steht: „Ticketverkauf an den Kassen täglich nur bis 10 Uhr.“ Darunter findet sich ein QR-Code, Verweis auf eine Website, wo man mit Paypal, Kreditkarte, Google und Apple Pay bezahlen kann. Die Familie verlässt den Eingangsbereich, der Vater zückt sein Smartphone und tippt konzentriert darauf herum.

Dann kommt Petra an die Reihe. „Nur mit Onlineticket“, sagt der Sicherheitsdienstleister. Petra hat aber kein Smartphone, mit dem sie sich ein solches kaufen könnte. Was nun? „Dann müssen Sie wieder nach Hause gehen“, sagt er. Die 66-Jährige dreht wortlos um.

In fünf Berliner Freibädern gilt die Onlineticketregel seit Anfang Juni. Die Initiative „Freibad einfach für alle“¹ kämpft dagegen mit einer Unterschriftensammlung. Den Aktivist:innen sind angeblich viele Fälle von Menschen begegnet, die nicht ins Freibad durften, weil ihr Handyakku leer war oder das Guthaben für mobile Daten aufgebraucht. Schwierig bis unmöglich werde das Schwimmen für Kinder und Jugendliche. „Sie haben weder Kreditkarte noch PayPal-Konto, die für den Kauf des Online-Tickets erforderlich sind. Oder für ältere Menschen, die keine Erfahrung mit Internet-Bestellungen haben“, so die Kampagnenseite.

Petra wird immer öfter ausgeschlossen

Petra, pensionierte Lehrerin, ist empört. Gar nicht so sehr darüber, dass sie jetzt nicht ins Schwimmbad darf, sondern weil dies ein Beispiel von vielen ist, mit denen sich die Welt nach und nach von ihr entfernt. Im Park neben dem Freibad, mit Blick auf den Sprungturm und Freibadlärm im Hintergrund, erzählt sie, was das für sie bedeutet.

Quelle: <https://netzpolitik.org/2024/ki-kann-keine-literatur-wert-menschlicher-uebersetzung/>

Anmerkungen

- 1 <https://literaturuebersetzer.de/berufspraktisches/umfragen-studien/vdue-honorarumfragen/>
- 2 <https://literaturuebersetzer.de/aktuelles/worterben-ergebnisse/>
- 3 <https://www.kunstoffonds.de/aktuelles/details/geplante-etatkuerzungen-im-haushalt-2025-spd-bundestagsfraktion-steht-an-der-seite-der-bundeskulturfonds>
- 4 <https://janinemalz.de/>



Die Bahncard nur noch mit Online-Account.

Quelle: Mullana, CC-BY 4.0

Viele Kulturveranstaltungen muss man übers Internet buchen. Zuletzt hat eine Freundin die Tickets gekauft, jetzt war Petra schon lang nicht mehr aus. Arztbesuche versucht sie zu vermeiden, „weil es oft nur noch digital Termine gibt“. Petra kann keine Bahncard nutzen, die gibt es nur noch mit Kundenkonto mit Mail-Adresse. Und ab Sonntag muss Petra, wenn sie Bus fahren will, vorher in einem Zeitungsladen Tickets kaufen. Beim Fahrer darf sie dann nicht mehr bar bezahlen.

Petra hat nicht nur kein Smartphone, sie hat auch kein Internet an ihrem Heim-PC. Sie nutzt kein Onlinebanking, sondern Überweisungsträger, die Bankkarte nur, um Bargeld zu holen. Sie verweigert ihre Anbindung an die digital vernetzte Welt, wo es geht. Für jemanden, der sich nicht im Internet bewegt, kann Petra erstaunlich informiert erklären warum. „Die Techgiganten wollen Daten und die kriegen sie auch. Und die haben Hintertüren für Geheimdienste. Und diese Türen finden auch Cyberkriminelle.“, sagt sie.

Petra ist ein Early Adopter. Sie hat schon Mitte der 1980er-Jahre einen Computerkurs an der Volkshochschule gemacht und war beeindruckt. „Wenn man sich verschrieben hat, konnte man das korrigieren!“ Später hat sie dann an ihrem ersten eigenen Com-

puter oft stundenlang Solitär gespielt. „Und dann dachte ich: Das hält mich irgendwie fest. Das will ich nicht.“ Seitdem nutze sie das Gerät nur noch zum Schreiben.

Entfremdung der Menschen voneinander und von der Natur

Petra hält nichts von Social-Media-Freundschaften. Sie findet, das Internet zerstöre gesellschaftliche Strukturen. „Es wird kaum mehr kommuniziert. Die meisten Menschen laufen nur noch mit dem Smartphone in der Hand herum oder sind verstöpselt. Da werden andere Menschen zum Teil umgestoßen aus Unachtsamkeit.“

Für eine demokratische Gesellschaft sei es wichtig, dass Menschen sich gegenseitig wahrnehmen. „Ich bin so aufgewachsen, dass man einander anguckt und das ist kaum noch da. Wenige reden noch miteinander. Das macht was mit den Menschen. Viele sind erschöpft und krank.“ Sie konstatiert eine Entfremdung der Menschen voneinander und auch von Umwelt und Natur.

Petra ist eine von vielen. Allein in der Altersgruppe zwischen 16 und 74 sind in Deutschland drei Millionen Menschen offline, so das *Statistische Bundesamt* für das Jahr 2023². Einige sind es freiwillig wie Petra. Andere haben keine andere Wahl, etwa weil die nötigen Geräte nicht ausreichend barrierefrei für sie nutzbar sind. Fast zwei Drittel der Menschen über 80 Jahren sind offline, so die Studie „Hohes Alter in Deutschland“³ für das Jahr 2022. Laut *Paritätischem Gesamtverband*⁴ hat ein Fünftel der arbeitslosen Menschen keinen Internetanschluss.

Demokratie braucht Teilhabe

Diese vielen Menschen ohne Internetzugang stehen einem Gesellschafts- und Wirtschaftssystem gegenüber, das die digitale Schnittstelle in beinahe allen Bereichen gegenüber dem persönlichen Kontakt priorisiert. Digitalisierung im Dienste der Effizienz. Die Berliner Bäderbetriebe schreiben zur Onlineticketpflicht: „Wir möchten, dass ihr möglichst ohne lange Wartezeiten in die Bäder kommt. Deshalb setzen wir zunehmend auf Digitalisierung.“

Doch Demokratie braucht Teilhabe. Sie muss alle mitnehmen. Auch die ohne Internetzugang. Teilhabe beginnt nicht erst in der Wahlkabine, sondern auch im Swimmingpool.

Das Europäische Parlament forderte deshalb 2022 in einer Entschließung zur Digitalen Kluft⁵, „dass viele tägliche Dienste eine nicht digitale Lösung bieten sollten, um den Bedürfnissen der

jenigen Bürger gerecht zu werden, die nicht über die für die Nutzung von Online-Diensten erforderlichen Fähigkeiten oder Kenntnisse verfügen, die Dienste offline nutzen möchten oder die keinen Zugang zu digitalen Geräten und Anwendungen haben.“

Eine analoge Option

Aktuell fordert eine Unterschriftenaktion von *Digitalcourage*⁶ ein „Recht auf Leben ohne Digitalzwang“. Mehr als 27.500 Menschen haben bereits signiert. Die Aktion läuft von Mai 2024 bis Mai 2025 und soll das Recht auf Digitalfreiheit ins Grundgesetz bringen. Damit soll eine Ausweitung der Überwachung verhindert werden und Teilhabe und gesellschaftliche Resilienz gestärkt.

Denn wenn mal was schiefgeht mit dem digitalen System, wird es plötzlich dringend, eine analoge Option bereitzuhaben. Außerdem ist, glaubt man zumindest Petra, das analoge Leben an sich schon wertvoll. „Es ist entspannter und verbindlicher. Man kann seine eigenen Empfindungen viel besser wahrnehmen, weil sie dann den Raum und die Zeit haben, bewusst zu werden.“ Sie empfiehlt, dabei auch an die Umwelt zu denken: „Was eine Serverfarm an Strom, sauberem Wasser und seltenen Erden benötigt, ist enorm.“

Quelle: <https://netzpolitik.org/2024/digitalzwang-wie-onlinepflicht-menschen-ausschliesst/>

Anmerkungen

- <https://www.openpetition.de/petition/online/freibad-einfach-fuer-alle-gegen-ausschluss-durch-online-ticket-zwang-und-ausweispflicht>
- https://www.destatis.de/DE/Presse/Pressemitteilungen/Zahl-der-Woche/2024/PD24_15_p002.html
- <https://www.bmfsfj.de/bmfsfj/aktuelles/alle-meldungen/ein-drittel-der-hochaltrigen-nutzt-das-internet-195818>
- <https://www.der-paritaetische.de/alle-meldungen/neue-studie-armut-fuehrt-zu-digitaler-ausgrenzung/>
- https://www.europarl.europa.eu/doceo/document/TA-9-2022-0438_DE.html
- <https://civi.digitalcourage.de/recht-auf-leben-ohne-digitalzwang>
- <mailto:martin.schwarzbeck@netzpolitik.org>
- <https://keys.openpgp.org/search?q=martin.schwarzbeck@netzpolitik.org>
- <https://kollektiva.social/@YoshiXYZ>



Martin Schwarzbeck

Martin Schwarzbeck ist seit 2024 Redakteur bei netzpolitik.org. Er hat Soziologie studiert, als Journalist für zahlreiche Medien gearbeitet, von ARD bis taz, und war zuletzt lange Redakteur bei Berliner Stadtmagazinen, wo er oft Digitalthemen aufgegriffen hat. Martin interessiert sich für Machtstrukturen und die Beziehungen zwischen Menschen und Staaten und Menschen und Konzernen. Ein Fokus dabei sind Techniken und Systeme der Überwachung, egal ob von Staatsorganen oder Unternehmen.

Kontakt: E-Mail⁷ (OpenPGP⁸), Mastodon⁹ Sachbücher aus dem Englischen, Italienischen und Niederländischen ins Deutsche.

Autoritäre Zeitenwende, schlüsselfertig

30. August 2024 – Nach dem Messerangriff in Solingen überbieten sich Politiker:innen mit Maßnahmen und Forderungen. Das ist falsch und gefährlich, denn es bereitet autoritären Strukturen einen fruchtbaren Boden. Ein Kommentar.

Politiker:innen der grünen Regierungspartei rufen eine „Zeitenwende in der Innenpolitik“¹ herbei. Unter den Wünschen: mehr Befugnisse für Polizei und Geheimdienste, mobile Grenzkontrollen und effizientere Abläufe dafür, „dass aus der möglichen eine tatsächliche Abschiebung wird“.

Kurz darauf verkündet die Regierung ein Maßnahmenpaket mit mehr Gesichtserkennung², Big-Data-Analysen und anlasslosen Kontrollen. Und natürlich: mehr Abschiebungen und noch weniger Rechten für Noch-nicht-Abgeschobene. Vielleicht bei Brot und Wasser im Abschiebeknast, bis sie endlich weg sind. Tags darauf die Meldung: 28 straffällige Afghanen sitzen im Flieger ins Taliban-Regime. Horst Seehofer, der sich einst 69 Abschiebungen zu seinem 69. Geburtstag³ wünschte, darf sich wieder jung fühlen.

Kein autoritärer Traum

Das ist kein autoritärer Traum, das ist die Realität in Deutschland im August 2024. Ein paar Tage, bevor in zwei Bundesländern Landtagswahlen stattfinden, bei denen die rechtsradikale AfD stärkste Kraft werden könnte. Ein paar Tage nach einem wohl islamistisch motivierten Messerangriff in Solingen. Ein terroristischer Akt oder auch ein Angriff auf unsere offene und freie Gesellschaft, wie Politiker:innen bei so etwas gerne sagen. „Diese freie Gesellschaft lässt sich nicht niederringen“, behauptete Ministerpräsident Hendrik Wüst (CDU) kurz nach der Tat⁴. Doch genau das passiert im Moment.

Während die Rechtsradikalen nach der Macht greifen, üben sich die verbliebenen Demokraten darin, den Staat für sie schlüsselfertig vorzubereiten. Es ist noch rund ein Jahr bis zur Bundestagswahl und die einst angetretene Fortschrittskoalition für eine „moderne, freie Gesellschaft“ trägt mit dem Presslufthammer Freiheitsrechte ab, als gäbe es einen Wettlauf zu gewinnen.

Dabei ist eine Brandmauer gegen den Faschismus mehr als nicht mit den Rechtsradikalen zusammenzuarbeiten. Sie besteht auch darin, nicht deren politische Agenda das eigene Handeln diktieren zu lassen.

Wo ist die progressive Politik?

Denn damit bereiten Politiker:innen nicht nur rechten und autoritären Tendenzen den Boden. Sie entziehen auch den Menschen Stück für Stück die progressiven, parteipolitischen Optionen, die noch bereit dazu sind, danach zu suchen. Gerade im Angesicht der anstehenden Bundestagswahlen ist das ein schwerer Fehler.

Es gibt sie auch, die Forderungen nach besserer psychosozialer Versorgung, nach besseren Integrationsmaßnahmen statt Abschiebe-Politik, nach Aufklärung. Doch Gehör finden sie zu wenig. Wir müssen sie lauter machen, damit sie nicht untergehen im Überbietungswettbewerb⁵ derer, denen nicht anderes einfällt, als nach Kontrolle zu schreien.

Gewiss, schnell und effektiv sind die leisen Forderungen nicht. Doch eine freie und offene Gesellschaft zu erhalten und zu fördern, ist eine Aufgabe für die Ewigkeit. Eine Demokratie abzubauen hingegen, das geht schnell.

Quelle: <https://netzpolitik.org/2024/massnahmen-nach-solingen-autoritaere-zeitenwende-schlusselfertig/>

Anmerkungen

- <https://irene-mihalic.de/berlin/innere-sicherheit/es-ist-an-der-zeit-die-zeitenwende-endlich-auch-in-der-innenpolitik-entschlossen-umsetzen>
- <https://netzpolitik.org/2024/sicherheitspaket-der-bundesregierung-ueberwachung-wie-sie-buerger-erwarten/>
- <https://www.spiegel.de/politik/deutschland/seehofer-69-abschiebungen-zum-69-geburtstag-a-1217747.html>
- <https://www.tagesspiegel.de/politik/bei-besuch-des-tatorts-in-solingen-scholz-kündigt-rasche-verschärfung-des-waffenrechts-an-12255869.html>
- <https://netzpolitik.org/2024/messerkriminalitaet-scharfe-debatte-stumpfe-argumentation/>
- <mailto:anna@netzpolitik.org>
- <https://keys.openpgp.org/search?q=anna@netzpolitik.org>
- <https://mastodon.social/@annskaja>



Anna Biselli

Anna Biselli ist Co-Chefredakteurin bei netzpolitik.org. Sie interessiert sich vor allem für staatliche Überwachung und Dinge rund um digitalisierte Migrationskontrolle.

Kontakt: E-Mail⁶ (OpenPGP⁷), Mastodon⁸, Telefon: +49-30-5771482-42 (Montag bis Freitag jeweils 8 bis 18 Uhr).

Macht endlich wirklich etwas gegen Staatstrojaner

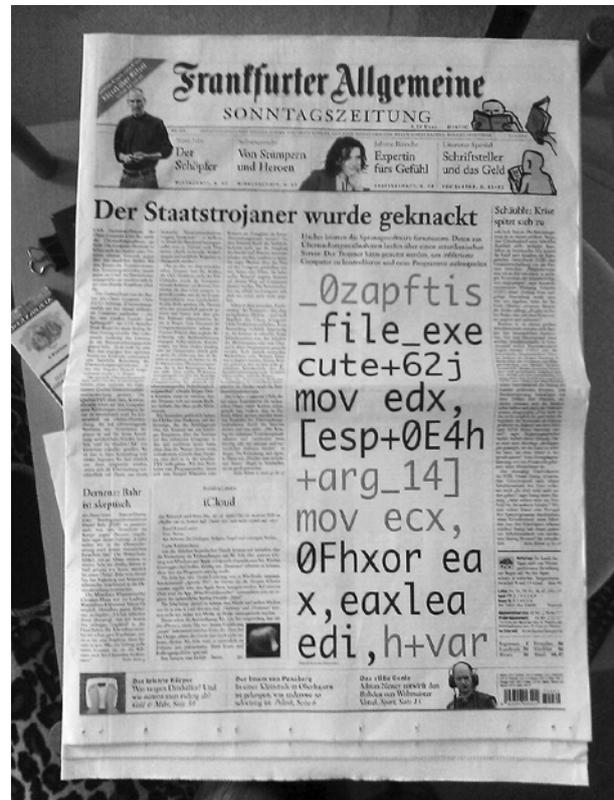
3. September 2024 – *Genug mit Verzögern und sachten Empfehlungen: Ein Bündnis aus Gruppen der Zivilgesellschaft will Taten gegen Spionagesoftware sehen. Es fordert von der neuen EU-Kommission klare Regeln für den Einsatz solcher Software.*

Eine Gruppe an zivilgesellschaftlichen Organisationen fordert mit einem heute veröffentlichten Statement¹ mehr Taten gegen Staatstrojaner. Die Spionageprogramme sollen stark eingeschränkt werden, die kommerzielle Entwicklung soll ganz verboten werden. Bis es neue Regeln gibt, sollen überhaupt keine Staatstrojaner mehr entwickelt werden dürfen.

Hintergrund für die Forderungen ist der Pegasus-Skandal vor inzwischen zwei Jahren. In dessen Rahmen wurde bekannt, dass auch EU-Regierungen mit Staatstrojanern Oppositionelle und Journalist:innen überwachten. Um diesen Skandal aufzuarbeiten, richtete das Europäische Parlament einen Untersuchungsausschuss ein. Den hat netzpolitik.org ausführlich begleitet².

Die praktischen Konsequenzen des Ausschusses waren jedoch zunächst gleich null. Die meisten Mitgliedstaaten versteckten sich hinter der Ausrede, es gehe bei ihren Spähaktionen um Fragen der nationalen Sicherheit, in die die EU nicht eingreifen darf.

Spanien eröffnete zwar 2022 ein Verfahren, das wurde aber wegen der fehlenden Kooperation Israels eingestellt. Dort sitzt das Unternehmen hinter dem Trojaner *Pegasus*, die *NSO Group*. Anfang dieses Jahres nahm dann in Polen eine parlamentarische Untersuchungskommission³ Fahrt auf. Die spanische Untersuchung wurde wiedereröffnet⁴, nachdem französische Behörden neue Informationen übergeben hatten. In Griechenland erklärte dagegen der Oberste Gerichtshof den Skandal einfach für beendet⁵.



Bundestrojaner alias Ozapftis auf der Titelseite der Frankfurter Allgemeinen Sonntagszeitung, Foto: Udo Springfield, CC BY 2.0

Mitgliedstaaten mauern, Kommission verzögert

Die EU-Kommission reagierte während all dessen ausweichend⁶ und lieferte keine konkreten Vorschläge, wie die Situation verbessert werden könnte.

„Die Antwort der Kommission auf die Ergebnisse des Pegasus-Ausschusses hat die Erwartungen nicht erfüllt“, sagte Silvia Lorenzo Perez zu netzpolitik.org. Sie arbeitet beim *Center for Democracy and Technology Europe* (CDT) zu Spionagesoftware und Menschenrechten. „Von der Leyen und die zuständigen Kommissar:innen haben nicht die Führung gezeigt, die nötig gewesen wäre, um für die Werte der EU zu kämpfen und Mitgliedstaaten zur Verantwortung zu ziehen“, sagte sie.

Die Kommission arbeitet gerade noch an einem Text⁷, mit dem sie auf den Skandal reagieren will. Der soll aber nur Empfehlungen an die Staaten enthalten, keine Verpflichtungen – was für starke Kritik aus dem Ausschuss sorgte. Seit der Ankündigung habe es außerdem keinerlei Fortschritt gegeben, sagt Lorenzo Perez. „Wir hoffen, dass die Verzögerung nicht in schwachen Empfehlungen mündet und dass die Kommission so hart sein wird, wie die Lage es verlangt.“

Es braucht eine grundlegende Reform

Zusammen mit anderen Organisationen wie *European Digital Rights* und *Access Now* fordert CDT nun, dass Mitgliedstaaten und EU-Kommission endlich tätig werden. Die EU-Institutionen werkeln gerade nach der Europawahl an ihrer Besetzung für die nächsten fünf Jahre. In Brüssel bringen deshalb Interessenverbände aller Richtungen ihre Forderungen vor, womit sich die EU in dieser Zeit beschäftigen soll.

Die Koalition fordert, dass die Kommission die Rahmenbedingungen für Spionagesoftware in der EU grundlegend umbauen soll. Software, die zu stark in Grundrechte eingreift, soll in Europa nicht mehr hergestellt, exportiert, verkauft, importiert, aufgekauft, transferiert oder benutzt werden dürfen.

Bis diese Reform umgesetzt ist, fordern die Organisationen ein komplettes Moratorium auf Staatstrojaner. Privatunternehmen sollen gar keine kommerzielle Spionagesoftware mehr herstellen dürfen. Trojaner sollen außerdem nicht mehr so einfach aus der EU exportiert werden dürfen – dazu soll es eine Garantie brauchen, dass sie nicht für Menschenrechtsverletzungen genutzt werden.

Die Organisationen erwähnen besonders die ePrivacy-Verordnung. Dieses Gesetz plant die EU seit langem, die Mitgliedstaaten blockieren es aber seit Jahren⁸. Eine Einigung ist sehr unwahrscheinlich. In Brüssel wird deshalb momentan darüber geredet, den Vorschlag zurückzuziehen und einen neuen Aufschlag zu starten. Der solle dafür sorgen, dass private Kommunikation besser geschützt wird, fordert das Statement.

„Nationale Sicherheit“ soll eingegrenzt werden

Gute EU-Regeln helfen aber nicht, wenn sich die Mitgliedstaaten einfach darüber hinwegsetzen. Deshalb soll die Kommission auch überprüfen, ob sich die nationalen Regierungen an schon gültiges Recht halten. Wenn nicht, dann soll sie diese Regierungen verklagen und europäisches Recht durchsetzen.

Ein großes Problem ist, dass sich die Regierungen immer wieder hinter den Schutzschild der nationalen Sicherheit zurückziehen können. Die EU hat dann nichts mehr zu sagen. Um das etwas schwerer zu machen, soll die Kommission eine einheitliche Definition von nationaler Sicherheit durchsetzen und dafür sorgen, dass die Mitgliedstaaten sie nicht nur als leere Ausrede nutzen.

Die Mitgliedstaaten sollen wiederum aufhören, in jedes neue europäische Gesetz eine Ausnahme für ihre nationale Sicherheit hineinzuverhandeln. Das würde Bürger:innen weiteren Grundrechtsverletzungen aussetzen, heißt es in dem Statement. Stattdessen sollen sie dafür sorgen, dass Opfer von Staatstrojanern vor Gericht ihre Rechte verteidigen können.

Gute Worte haben die Organisationen nur für das Parlament. Das soll weiterhin überwachen, wie die Mitgliedstaaten Staatstrojaner einsetzen. Das Parlament sei mit der Europawahl zwar nach rechts gerückt, meint Silvia Lorenzo Perez. Viele der Abgeordneten, die sich gegen Staatstrojaner eingesetzt haben, seien aber wiedergewählt worden. „Wir erwarten von ihnen, dass sie ihren Kampf in der neuen Legislaturperiode fortsetzen, besonders weil viele Abgeordnete aus fast allen Fraktionen selber Opfer von Spionagesoftware geworden sind“, sagt sie.

Parlament hat noch eine große Chance

Die Zivilgesellschaft hat keine schlechten Chancen mit dem Versuch, den Pegasus-Skandal noch einmal auf der Agenda nach oben zu schieben: Finnland hat für die zweite Kommission Ursula von der Leyen eine neue Kommissarin nominiert, Henna Virkkunen.

Virkkunen sitzt gerade noch im Europaparlament – wo sie in der letzten Legislaturperiode Mitglied im Pegasus-Ausschuss war.

Sie hatte auch zu verschiedenen anderen Digitalthemen gearbeitet, besonders zu Cybersicherheit. Es könnte deshalb gut sein, dass sie in der neuen Kommission einen Digitalposten bekommt, und damit Einfluss darauf, wie sich die neue Kommission zu Spionagesoftware positionieren wird.

Und das Parlament könnte auch noch einmal Druck machen, findet Sophie in 't Veld. Sie saß bis zur vergangenen Wahl lange im Europaparlament, unter anderem im Pegasus-Ausschuss. Sie weist darauf hin, dass die neuen Kandidat:innen für die Kommission die Zustimmung des Parlaments brauchen. Die Abgeordneten sollten deshalb einer Kandidatin nur zustimmen, wenn diese sich verpflichtet, die Empfehlungen des Parlaments zu Staatstrojanern umzusetzen, fordert in 't Veld. Das sieht auch Lorenzo Perez so.

„Es wäre besser gewesen, wenn das Parlament das bei der Bestätigung von von der Leyen getan hätte, aber diese Gelegenheit hat es leider verpasst“, so in 't Veld zu netzpolitik.org. Wenn das Parlament seinen Einfluss jetzt nicht nutze, dann werde es danach keinen mehr haben. „Jetzt ist der Zeitpunkt, wo die Abgeordneten zeigen sollen, dass sie es ernst meinen.“

Quelle: <https://netzpolitik.org/2024/forderung-an-neue-eu-kommission-macht-endlich-wirklich-etwas-gegen-staatstrojaner/>

Anmerkungen

- 1 <https://cdt.org/insights/civil-society-joint-statement-on-the-use-of-surveillance-spyware-in-the-eu-and-beyond/>
- 2 <https://netzpolitik.org/tag/pegasus/>
- 3 <https://netzpolitik.org/2024/pegasus-ueberwachungsskandal-polnische-untersuchungskommission-nimmt-arbeit-auf/>
- 4 <https://www.dw.com/en/spain-court-reopens-investigation-in-pegasus-spying-scandal/a-68901546>
- 5 <https://netzpolitik.org/2024/predator-staatsanwaeltin-erklaert-griechischen-abhoer-skandal-fuer-beendet/>
- 6 <https://netzpolitik.org/2023/unzufrieden-mit-der-kommission-eu-abgeordnete-erwaegen-zweiten-staatstrojaner-ausschuss/>
- 7 <https://www.politico.eu/article/eu-commission-national-security-does-not-justify-spying-document/>
- 8 <https://netzpolitik.org/2023/eprivacy-verordnung-herzstillstand-fuer-das-digitale-briefgeheimnis/>
- 9 <https://maxhenning.eu/>
- 10 <mailto:max@maxhenning.eu>
- 11 <https://keys.openpgp.org/search?q=max%40maxhenning.eu>
- 12 <https://darmstadt.social/@zarasophos>
- 13 <https://bsky.app/profile/zarasophos.bsky.social>
- 14 <https://twitter.com/zarasophos>



Maximilian Henning

Maximilian Henning ist freier EU-Korrespondent zu Digitalthemen in Brüssel. Nebenher bastelt er auch gern an Datenanalysen und postet auf seiner Webseite⁹ darüber, wenn etwas Interessantes herauskommt.

Kontakt: E-Mail¹⁰ (OpenPGP¹¹), Mastodon¹², Bluesky¹³, Twitter¹⁴

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	1 400 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	Jörg Pohle und Stefan Hügel
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	Stefan Hügel, CC BY
Druck	Girzig+Gottschalk GmbH, Bremen Heftinhalt auf 100 % Altpapier gedruckt.



Druckprodukt mit finanziellem
Klimabeitrag
ClimatePartner.com/12164-2404-1001



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 Abonnent:innen, Adressänderungen dem FIfF-Büro möglichst umgehend mitzuteilen.

Aktuelle Ankündigungen

(mehr Termine unter www.fiff.de)

FIfF-Konferenz 2024 – „Nachhaltigkeit in der IT green coding – open source – green by IT“
25.–27. Oktober 2024 Hochschule Bremerhaven

FIfF-Kommunikation

4/2024 „Künstliche Intelligenz zwischen euphorischen Erwartungen und dystopischen Szenarien“

Margita Zallmann, Hans-Jörg Kreowski und Stefan Hügel
Redaktionsschluss: 2. November 2024

1/2025 „#FIfF-Konferenz 2024“

Karin Vosseberg, Ulrike Erb, Oliver Radfelder und Lars Fischer
Redaktionsschluss: 2. Februar 2025

Zuletzt erschienen:

3/2023 IT-Gestaltung für Gute Arbeit

4/2023 Wissenschaft für den Frieden

1/2024 FIfF-Konferenz 2023

2/2024 40 Jahre FIfF – denkwürdige Zeiten

W&F – Wissenschaft & Frieden

4/23 40 Jahre Wissenschaft & Frieden

1/24 Konflikte im „ewigen“ Eis

2/24 Fokus Mittelmeer

3/24 Widerstehen – Widersetzen

vorgänge – Zeitschrift für Bürgerrechte und Gesellschaftspolitik

#242 Künstliche Intelligenz

#243 Kritische Kriminalpolitik

#244 Identitätspolitik

#245/246 Klima(un)gerechtigkeit

DANA – Datenschutz-Nachrichten

4/23 Internet der Dinge

1/24 DSGVO und BDSG und Datenschutzaufsicht

2/24 Gesundheitsdaten

3/24 Nach der Europawahl

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 **E..I..f..F..**



„Frieden“ schaffen – mit immer mehr Waffen

**Grabsteine auf dem US-Nationalfriedhof in Arlington, Virginia,
stellvertretend für viele andere**

Foto: Fronl, CC BY-SA 4.0, https://commons.wikimedia.org/wiki/File:Tombstones_at_Arlington_National_Cemetery.jpg

Nutzungshinweise

Die vorliegende Datei wird im Rahmen der Mitgliedschaft des FfF e. V. oder eines Abonnements der FfF-Kommunikation zur Verfügung gestellt.

Die Einspeisung in Datenbanksysteme, Listen, Blogs oder die Bereitstellung der Datei zum Download durch Dritte wird ausdrücklich untersagt – die Datei dient ausschließlich dem privaten unbegrenzten Gebrauch durch die Mitglieder und die Abonnent:innen.